Nortel Ethernet Routing Switch 5500 Series

Configuration-IP Routing Protocols

NN47200-503 (217465-C)

Document status: Standard
Document version: 03.01
Document date: 27 August 2007

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document a re believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks .

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Nortel Networks software license agreement

This Software License Agreement ("License Agreement") is between you, the end user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other

reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a) If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b) Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c) Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d) Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e) The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f) This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Revision History

Date Revised	Version	Reason for revision
July 2005	1.00	New document for Software Release 4.2.
July 2006	2.00	Document updated for Software Release 5.0.
August 2007	3.01	updated for Software Release 5.1

Contents

Preface

This document provides information and instructions on the configuration of IP Routing on the 5500 Series Nortel Ethernet Routing Switch. Consult any documentation included with the switch and the product release notes (see "Related publications" (page 10)) for any errata before beginning the configuration process.

Nortel Ethernet Routing Switch 5500 Series

"5500 Series Switch Platforms" (page 9)outlines the switches that are part of the 5500 Series of Nortel Ethernet Routing Switches

5500 Series Switch Platforms

5500 Series Switch Model	Key Features
Nortel Ethernet Routing Switch 5510-24T	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5510-48T	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5520-24T-PWR	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5520-48T-PWR	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5530-24TFD	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains twelve shared SFP ports and two XFP ports.

Related publications

For more information about the management, configuration, and use of the Nortel Ethernet Routing Switch 5500 Series, refer to the publications listed in"Nortel Ethernet Routing Switch 5500 Series Documentation" (page 10).

Nortel Ethernet Routing Switch 5500 Series Documentation

Title	Description	Part Number
Nortel Ethernet Routing Switch 5500 Series Release 5.1 Installation	Instructions for the installation of a switch in the Nortel Ethernet Routing Switch 5500 Series. It also provides an overview of hardware key to the installation, configuration, and maintenance of the switch.	NN47200-300
Nortel Ethernet Routing Switch 5500 Release 5.1 Series Configuration - System	Instructions for the general configuration of switches in the 5500 Series that are not covered by the other documentation.	NN47200-500
Nortel Ethernet Routing Switch 5500 Release 5.1 Series Configuration - Security	Instructions for the configuration and management of security for switches in the 5500 Series.	NN47200-501
Nortel Ethernet Routing Switch 5500 Series Release 5.1 Configuration - VLANs, Spanning Tree, and Link Aggregation	Instructions for the configuration of spanning and trunking protocols on 5500 Series switches	NN47200-502
Nortel Ethernet Routing Switch 5500 Release 5.1 Configuration - IP Routing Protocols	Instructions for the configuration of IP routing protocols on 5500 Series switches.	NN47200-503
Nortel Ethernet Routing Switch 5500 Series Release 5.1 Configuration - Quality of Service	Instructions for the configuration and implementation of QoS and filtering on 5500 Series switches.	NN47200-504
Nortel Ethernet Routing Switch 5500 Release 5.1 Configuration - System Monitoring	Instructions for the configuration, implementation, and use of system monitoring on 5500 Series switches.	NN47200-505

Title	Description	Part Number
Nortel Ethernet Routing Switch 5500 Series Release Notes - Release 5.1	Provides an overview of new features, fixes, and limitations of the 5500 Series switches. Also included are any supplementary documentation and document errata.	NN47200-400
Installing the Nortel Ethernet Redundant Power Supply 15	Instructions for the installation and use of the Nortel Ethernet RPS 15.	217070-A
DC-DC Converter Module for the Baystack 5000 Series Switch	Instructions for the installation and use of the DC-DC power converter.	215081-A
Nortel Ethernet Routing Switch 5500 Series Release 5.1 Installation - SFP	Instructions for the installation and use of SFP transceivers.	NN47200-302

You can access technical documentation online at the Nortel Technical Support web site, located at http://www.nortel.com/support. Use the following procedure to access documents on the Technical Support web site:

- If it is not already selected, click the **Browse product support** tab.
- From the list provided in the product family box, select **Nortel Ethernet Routing Switch**.
- From the product list, select the desired 5500 Series Switch.
- From the content list, select **Documentation**.
- Click **Go**.

You can view documents online, download them for future reference, or printed them. All documents available on the Technical Support web site are in Adobe Portable Document Format (PDF) format.

Finding the latest updates on the Nortel web site

The content of this documentation was current at the time of release. To check for updates to the documentation and software for the Nortel Ethernet Routing Switch 5500 Series, use the links provided in the following table.

Software	Nortel Ethernet Routing Switch 5500 Series Software
Documentation	"Nortel Ethernet Routing Switch 5500 Series Documentation" (page 10)

How to get help

If a service contract for the Nortel product has been purchased from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If a Nortel service program was purchased, contact Nortel Technical Support.

The following information is available online:

- contact information for Nortel Technical Support
- information about the Nortel Technical Solutions Centers
- information about the Express Routing Code (ERC) for your product

An ERC is available for many Nortel products and services. When an ERC is used, the call is routed to technical support personnel who specialize in supporting the service or product. The ERC for a particular product or service is available online.

The main Nortel support portal is available at http://www.nortel.com/support.

An Introduction to IP Routing Protocols

This chapter provides an introduction to IP routing and IP routing protocols used in the Nortel Ethernet Routing Switch 5500 Series. Subsequent chapters will provide a more detailed description of switch capabilities and configuration procedures.

IP routing

To configure IP routing on the Nortel Ethernet Routing Switch 5500 Series, use virtual local area networks (VLAN) to create virtual router interfaces by assigning an IP address to the VLAN. This section discusses this concept in depth.

For a more detailed description about VLANs and their use, consult *Nortel Ethernet Routing Switch 5500 Series Release 5.1 Configuration - VLANs, Spanning Tree, and Link Aggregation*.

IP addressing

An IP version 4 (IPv4) address consists of 32 bits expressed in a dotted-decimal format (XXX.XXX.XXX.XXX). The IPv4 address space is divided into classes, with classes A, B, and C reserved for unicast addresses and accounting for 87.5 percent of the 32-bit IP address space. Class D is reserved for multicast addressing. " IP address classifications" (page 13)lists the breakdown of the IP address space by address range and mask.

IP address classifications

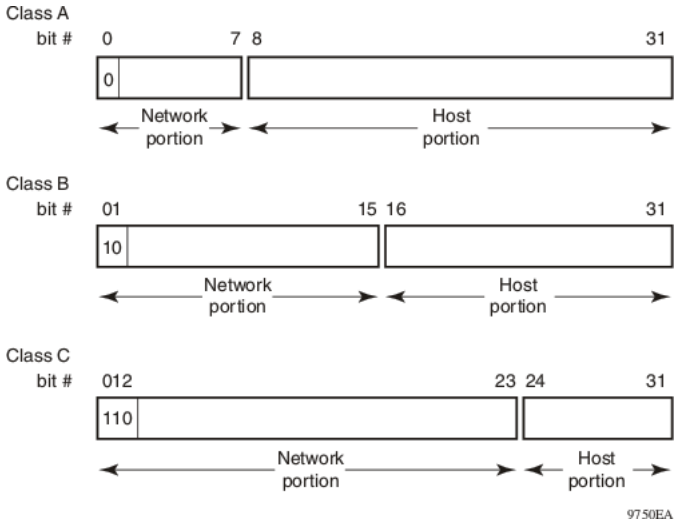
Class	Address Range	Mask	Number of Networks	Nodes per Network
A	1.0.0.0 - 127.0.0.0	255.0.0.0	127	16,777,214
Note: Although technically part of Class A addressing, network 127 is reserved for loopback.				
B	128.0.0.0 - 191.255.0.0	255.255.0.0	16,384	65,534
C	192.0.0.0 - 223.255.255.0	255.255.255.0	2,097,152	255

Class	Address Range	Mask	Number of Networks	Nodes per Network
D	224.0.0.0 - 239.255.255.254			
Note: Class D addresses are primarily reserved for multicast operations although the addresses 224.0.0.5 and 224.0.0.6 are used by OSPF and 224.0.0.9 is used by RIP.				
E	240.0.0.0 - 240.255.255.255			
Note: Class E addresses are reserved for research purposes.				

To express an IP address in dotted-decimal notation, each octet of the IP address is converted to a decimal number and separated by decimal points. For example, the 32-bit IP address 10000000 00100000 00001010 10100111 is expressed in dotted-decimal notation as 128.32.10.167.

Each IP address class, when expressed in binary notation, has a different boundary point between the network and host portions of the address, as illustrated in "Network and host boundaries in IP address classes" (page 14). The network portion is a network number field from 8 through 24 bits. The remaining 8 through 24 bits identify a specific host on the network.

Network and host boundaries in IP address classes



Subnet addressing

Subnetworks (or subnets) are an extension of the IP addressing scheme. Subnets allow an organization to use one IP address range for multiple networks. Subnets are two or more physical networks that share a common network-identification field (the network portion of the 32-bit IP address).

A subnet address is created by increasing the network portion to include a subnet address, thus decreasing the host portion of the IP address. For example, in the address 128.32.10.0, the network portion is 128.32, while the subnet is found in the first octet of the host portion (10). A subnet mask is applied to the IP address and identifies the network and host portions of the address.

" Subnet masks for Class B and Class C IP addresses" (page 15)illustrates how subnet masks used with Class B and Class C addresses can create differing numbers of subnets and hosts. This example shows the use of the zero subnet, which is permitted on a Nortel Ethernet Routing Switch 5510.

Subnet masks for Class B and Class C IP addresses

Number of bits	Subnet Mask	Number of Subnets (Recommended)	Number of Hosts per Subnet
Class B			
2	255.255.192.0	2	16 382
3	255.255.224.0	6	8 190
4	255.255.240.0	14	4 094
5	255.255.248.0	30	2 046
6	255.255.252.0	62	1 022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1 022	62
11	255.255.255.224	2 046	30
12	255.255.255.240	4 094	14
13	255.255.255.248	8 190	6
14	255.255.255.252	16 382	2
Class C			
1	255.255.255.128	0	126
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Variable-length subnet masking (VLSM) is the ability to divide an intranet into pieces that match network requirements. Routing is based on the longest subnet mask or network that matches.

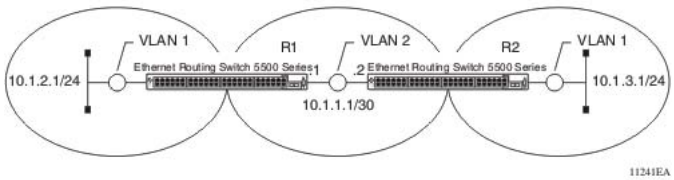
IP routing using VLANs

The Nortel Ethernet Routing Switch 5500 Series supports wire-speed IP routing between virtual LANs (VLAN). This type of routing is also referred to as virtual routing. When a virtual router interface is created for a specified VLAN, a specific IP address is associated with the specific VLAN. In this release, the Nortel Ethernet Routing Switch 5500 Series supports static routing, in which the identifiers of the devices being routed between are entered manually.

This virtual router interface does not have an association with any specified port or set of ports (it is called a virtual router interface because it is not associated with any particular port). The VLAN IP address can be reached through any of the ports in the VLAN specified as a virtual router interface, and the assigned IP address is the gateway through which packets are routed out of that VLAN. Routed traffic can be forwarded to another VLAN within the switch or stack of Nortel Ethernet Routing Switch 5500 Series.

Once routing is enabled on two VLANs by assigning IP addresses, routing can be performed between those two VLANs (refer to "IP routing with VLANs" (page 16)).

IP routing with VLANs



IP routing is enabled or disabled globally on the Nortel Ethernet Routing Switch 5500 Series. By default, IP routing is disabled.

Note: All IP routing parameters can be configured on the Nortel Ethernet Routing Switch 5500 Series before routing is actually enabled on the switch.

There is no longer a one-to-one correspondence between the physical port and the router interface, because a given port can belong to multiple VLANs. The VLANs may be configured for routing on the switch.

As with any IP address, virtual router interface addresses are also used for device management. For management over IP, any virtual router interface IP address can be used to access the switch as long as routing is enabled. When the Nortel Ethernet Routing Switch 5500 Series switch or stack is used without routing enabled, the Management VLAN is reachable only through the switch or stack IP address. With IP routing enabled on the switch or stack, any of the virtual router IP interfaces can be used for management over IP.

Once routing is enabled on the Nortel Ethernet Routing Switch 5500 Series switches, the Management VLAN behaves like all other routable VLANs. The IP address is reachable through any virtual router interface, as long as a route is available. Actually, all virtual router interfaces can be used as the Management VLAN over IP.

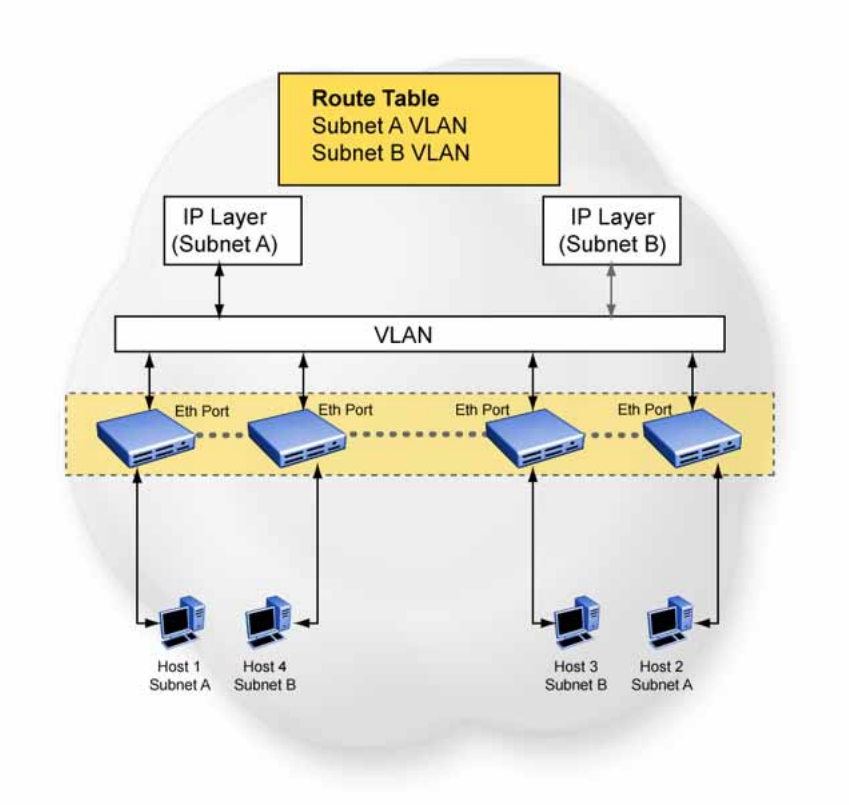
Multinetting

The Nortel Ethernet Routing Switch 5500 Series supports the definition and configuration of up to eight secondary interfaces on each VLAN (multinetting). With IP multinetting, you can associate multiple IP subnets with one VLAN. That is, connected hosts can belong to different IP subnets on the same VLAN.

Multinetting can be configured using the CLI or the Device Manager.

The following diagram illustrates a network with configured IP multinetting.

Network with Multinetting



You can configure a static route with the next hop on the secondary interface. You can also add static ARP for a given IP address in the same subnet of a secondary interface.

Here are some limitations when you are working with secondary interfaces:

- you can have a maximum of eight secondary interfaces on each VLAN
- you can have a total maximum of 256 IP interfaces (including primary and secondary)
- all of the secondary interfaces on a VLAN are enabled or disabled together. There is no provision for configuring the administrative state of the secondary IP interfaces individually.
- dynamic routing is not available for secondary IP interfaces
- secondary interfaces are not supported on brouters
- a primary IP interface must be in place before secondary IP interfaces can be added; secondary interfaces must be deleted before you can delete the primary

If secondary interfaces are configured on the management VLAN, routing cannot be disabled globally or on the management VLAN. Secondary IP interfaces on the management VLAN are purged from NVRAM when

- a unit leaves the stack and the switch does not have a manually configured IP
- the switch fails to get the IP address through the BootP mode

The following are not supported on secondary interfaces:

- DHCRP
- Proxy ARP
- UDP broadcast
- IPFIX
- VRRP, OSPF, RIP

For information about configuring secondary interfaces on VLANs, see "IP routing using VLANs" (page 16).

Brouter port

The Nortel Ethernet Routing Switch 5500 Series supports the concept of brouter ports. A brouter port is a single-port VLAN that can route IP packets as well as bridge all non-routable traffic. The difference between a brouter port and a standard IP protocol-based VLAN configured to do routing is that the routing interface of the brouter port is not subject to the spanning tree state of the port. A brouter port can be in the blocking state for non-routable traffic and still be able to route IP traffic. This feature removes any interruptions caused by Spanning Tree Protocol recalculations in routed traffic. A brouter port is actually a one-port VLAN; therefore, each brouter port decreases the number of available VLANs by one and uses one VLAN ID.

When a brouter port is created, the following actions are also taking place on the switch:

- A port-based VLAN is created.
- The brouter port is added to the new port-based VLAN.
- The PVID of the brouter port is changed to the VLAN ID of the new VLAN.
- The STP participation of the brouter port is disabled.
- An IP address is assigned to the brouter VLAN.

Management VLAN

Prior to Software Release 4.0, the Management VLAN was the only VLAN that was used to carry the management traffic, including Telnet, Web, SNMP, BootP and TFTP for the switch. The Management VLAN always exists on the switch and cannot be removed. All IP settings, including switch IP address, stack IP address, subnet mask and default gateway, apply only to the Management VLAN.

In this release of Nortel Ethernet Routing Switch 5500 Series, a regular Layer 2 (L2) VLAN behaves like a routable L3 VLAN if a pair of IP addresses and a MAC address are attached to the VLAN. When routing is enabled in L3 mode, every L3 VLAN is capable of doing routing as well as carrying the management traffic. Any L3 VLAN can be used instead of the Management VLAN to manage the switch.

Layer 2 versus Layer 3 mode

When the Nortel Ethernet Routing Switch 5500 Series is configured to route IP traffic between different VLANs, the switch is considered to be running in L3 mode; otherwise, the switch runs in L2 mode.

The L3 manager determines in which mode a switch or a stack should be run. The mode is determined based on the user settings and events. But the general rule is to select:

- L3 mode: if routing is turned on globally for the switch or stack.
- L2 mode: if routing is turned off globally for the switch or stack.

Routing and management

In L3 mode, the Management VLAN, as well as all other L3 VLANs, has the capability to route and carry the management traffic. In this release of the Nortel Ethernet Routing Switch 5500 Series, the settings apply to all L3 VLANs or only to the Management VLAN. "VLAN settings" (page 20)shows all possible settings and default settings for each type of VLAN.

VLAN settings

VLAN/Feature	Routing (default)	Management (Routing)	Default Route
Management VLAN (L2 mode)	Off	On	Yes (Management VLAN only)
Management VLAN (L3 mode)	On/off (on)	On	No
L3 VLAN	On/off (on)	On/off (on)	Yes (global)

Setting IP routing

To set IP routing (or L3 VLANs), take the following steps:

Step	Action
1	Enable IP routing globally.
2	Assign an IP address to the specific VLAN or brouter port.
3	Enable IP routing on the interface.

—End—

Refer to subsequent chapters in this document for detailed instructions on configuring IP routes.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP)

Network stations using the IP protocol need both a physical address and an IP address to transmit a packet. If a network station knows only a network host's IP address, the Address Resolution Protocol (ARP) enables the network station to determine a network host's physical address and bind the 32-bit IP address to a 48-bit MAC address. A network station can use ARP across a single network only, and the network hardware must support physical broadcasts.

If a network station wants to send a packet to a host but knows only the host's IP address, the network station uses ARP to determine the host's physical address as follows:

1. The network station broadcasts a special packet, called an ARP request, that asks the host at the specified IP address to respond with its physical address.
2. All network hosts receive the broadcast message.
3. Only the specified host responds with its hardware address.
4. The network station then maps the host's IP address to its physical address and saves the results in an address resolution table for future use.
5. The network station's ARP table displays the association of the known MAC addresses to IP addresses.

Note: The default timeout value for ARP entries is 6 hours.

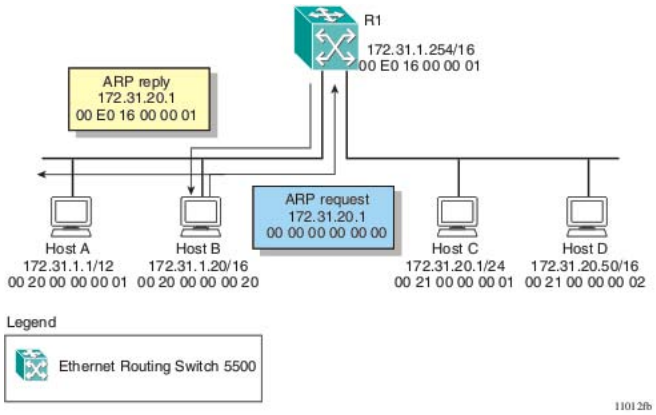
Static ARP entries can be created and individual ARP entries deleted.

Proxy Address Resolution Protocol (Proxy ARP)

Proxy ARP allows a network station to respond to an ARP request from a locally attached host or end station for a remote destination. It does so by sending an ARP response back to the local host with its own MAC address of the network station interface for the subnet on which the ARP request was received. The reply is generated only if the switch has an active route to the destination network.

The figure below is an example of proxy ARP operation. In this example, host C with a 24-bit mask appears to be locally attached to host B with a 16-bit mask, so host B sends an ARP request for host C. However, the 5500 Series switch is between the two hosts. To enable communication between the two hosts, the 5500 Series switch would respond to the ARP request with host C's IP address but with its own MAC address.

Proxy ARP Operation



Static routes

Once routable VLANs are created though IP address assignment, static routes can be created. Static routes allow for the manual creation of specific routes to a destination IP address. Static routes can also be used to specify a route to all networks for which there are no explicit routes in the Forwarding Information Base or the routing table. This static default route is a route to the network address 0.0.0.0 as defined by the IEEE RFC 1812 standard.

Because of their static nature, this type of solution is not scalable. Thus, in a large or growing network this type of route management may not be desirable. Also, static routes do not have the capacity to determine the failure of paths. Thus, a router can still attempt to use a path after it has failed.

Non-local static routes

The Nortel Ethernet Routing Switch 5500 Series supports the usage of non-local static routes. A non-local static route is almost identical to a static route with the exception that the next hop of the route is not directly connected to the network entity. Non-local static routes are useful in situations where there are multiple paths to a network and the number of static routes could be reduced by using only one route with a remote gateway.

Because of their static nature, this type of solution is not scalable. Thus, in a large or growing network this type of route management may not be desirable. Also, non-local static routes do not have the capacity to determine the failure of paths. Thus, a router can still attempt to use a path after it has failed.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a standard, dynamic routing protocol based on the Bellman-Ford (or distance vector) algorithm. It is used as an Interior Gateway Protocol (IGP). RIP allows routers to exchange information to compute routes through an IPv4-based network. The hop count, or distance, is used as a metric to determine the best path to a remote network or host. The hop count cannot exceed 15 hops (assuming a cost of one hop for each network).

RIP is defined in RFC 1058 for RIP version 1 and RFC 2453 for RIP version 2. The most significant difference between the two versions is that RIP version 2 supports subnet masks and next hop information in the RIP packet.

RIP operation

RIP uses User Datagram Protocol (UDP) data packets to exchange routing information. Each router maintains a routing table, which lists the optimal route to every destination in the system. Each router *advertises* its routing information by sending a routing information update at regular intervals. Neighboring routers use this information to recalculate their routing tables and retransmit the routing information. For RIP version 1, no mask information is exchanged; the natural mask is always applied by the router receiving the update. For RIP version 2, mask information is always included.

The sequence of processes governed by the routing algorithm is as follows:

1. When a router starts, it initializes the RIP data structures and then waits for indications from lower-level protocols that its interfaces are functional.
2. RIP advertisements are send on all the interfaces that are configured to send routing information.

3. The neighbors will send their routing tables and the new router will update its routing table based on the advertisements received.
4. From now on periodic updates are send by each router in the network to ensure a correct routing database.

If a router does not receive an update from another router within a timeout period, it deletes the routes served by the *nonupdating* router from its routing table. However, it keeps these routes temporarily in a *garbage list* and continues to advertise them with a metric of 16 for a *holddown* period, so that neighbors know that the routes are unreachable. If a valid update for a garbage route is received within the holddown period, the router adds the route back into its routing table. If no update is received, the router completely deletes all garbage list entries for the *nonupdating* router.

To prevent routing loops and to promote fast convergence, RIP uses the mechanisms of split horizon, with or without poisoned reverse, and triggered updates. Simple split horizon means that IP routes learned from a neighbor are not advertised back in updates to that neighbor. Split horizon with poisoned reverse means that these routes are advertised back to the neighbor, but they are “poisoned” with a metric of 16, which represents infinite hops in the network. The receiver neighbor therefore ignores this route. Triggered updates means that a router is required to send update messages whenever it changes the metric for a route, even if it is not yet time for a regular update message.

RIP sends routing information updates every 30 seconds. These updates contain information about known networks and the distances (hop count) associated with each. For RIP version 1, no mask information is exchanged; the natural mask is always applied by the router receiving the update. Mask information is always included for RIP version 2.

If information about a network is not received for within the allotted timeout period (180 seconds by default), it is removed from the routing table and the route is moved to the garbage list . From the garbage list it will be advertised for the allotted holdown period (120 seconds by default) with metric set to infinity (16). These timers can be changed by configuring the RIP Interface Timeout Timer and Holddown Timer parameters.

RIP supports the following standard behavior:

- periodic RIP updates about effective best routes
- garbage collection
- split horizon with or without poisoned reverse
- triggered update for changed RIP routes
- unicast to the specific query requestor
- broadcast/multicast of regular and triggered updates

- subnet mask (RIP version 2)
- routing table update based on the received RIP message
- global update timer
- holddown timer and timeout timer per device and per interface
- cost per device and per interface

The Nortel Ethernet Routing Switch 5500 Series implementation of RIP also supports the following features:

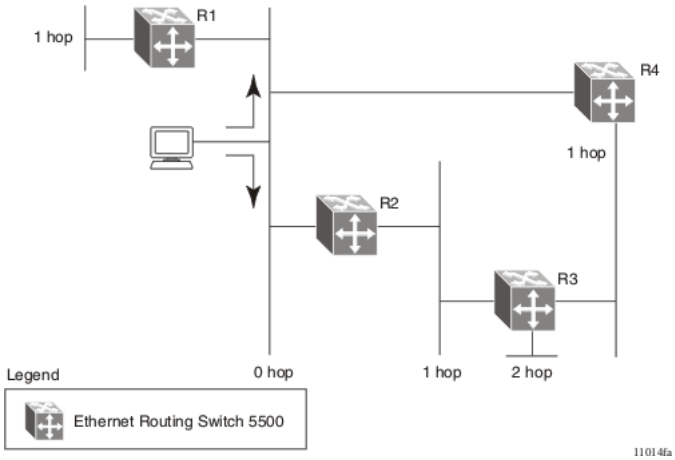
- in and out routing policies
- auto-aggregation (also known as *auto-summarization*) of groups of adjacent routes into single entries

Many RIP features are configurable. The actual behavior of the protocol depends on the feature configurations.

RIP metrics

RIP is known as a distance vector protocol. The vector is the network number and next hop, and the distance is the cost associated with the network number. RIP identifies network reachability based on cost, and cost is defined as hop count. The distance from one router to the next is considered to be one hop. This cost or hop count is known as the *metric* The illustration below depicts the hop counts between various units in a network.

RIP hop counts



A directly connected network has a metric of zero. An unreachable network has a metric of 16. Therefore, 15 hops or 15 routers is the highest possible metric between any two networks.

RIP Send and Receive Modes

RIP can be configured to use a number of different send and receive modes depending on the specifics of the network configuration. The following table lists the send and receive modes supported.

RIP send and receive modes

Send Mode	Description	Result
rip1comp	This mode is used to broadcast RIP version 2 updates using RFC 1058 route consumption rules. This is the default send mode for the Nortel Ethernet Routing Switch 5500 Series.	• Destination MAC is a broadcast, ff-ff-ff-ff-ff-ff • Destination IP is a broadcast for the network (for example, 192.1.2.255) • RIP Update is formed as a RIP version 2 update, including network mask • RIP version = 2
rip1	This mode is used to broadcast RIP updates that are compliant with RFC 1058.	• Destination MAC is a broadcast, ff-ff-ff-ff-ff-ff • Destination IP is a broadcast for the network (for example, 192.1.2.255) • RIP Update is formed as a RIP version 1 update, no network mask included • RIP version = 1
rip2	This mode is used to broadcast multicast RIP version 2 updates.	• Destination MAC is a multicast, 01-00-5e-00-00-09 • Destination IP is the RIP version 2 multicast address, 224.0.0.9 • RIP Update is formed as a RIP version 2 update including network mask • RIP version = 2
nosend	No RIP updates are sent on the interface.	None
Receive Mode	**Result**	

rip1OrRip2	RIP version 1 or RIP version 2 updates are accepted.
rip1	RIP version 1 and RIP version 1 compatible updates only are accepted.
rip2	RIP version 2 updates only are accepted.

Limitations

RIP has the following limitations:

- The protocol is limited to networks whose longest path is 15 hops.
- The protocol depends on counting to infinity to resolve certain unusual situations.
- The protocol uses fixed metrics (the hop number) to compare alternative routes, as opposed to real-time parameters such as measured delay, reliability, or load.
- RIP does not support address-less links.

Open Shortest Path First (OSPF) protocol

The Open Shortest Path First (OSPF) Protocol is an Interior Gateway Protocol (IGP) that distributes routing information between routers belonging to a single *autonomous system* (AS). Intended for use in large networks, OSPF is a link-state protocol which supports IP subnetting and the tagging of externally-derived routing information.

> ***Note:*** The Nortel Ethernet Routing Switch 5500 Series implementation of OSPF only supports broadcast and passive interfaces. Point-to-point and NBMA interfaces are not supported.

Overview

In an OSPF network, each router maintains a *link-state database* that describes the topology of the autonomous system (AS). The database contains the *local state* for each router in the AS, including the router's usable interfaces and reachable neighbors.

Each router periodically checks for changes in its local state and shares any changes detected by flooding *link-state advertisements* (LSAs) throughout the AS. Routers synchronize their topological databases based on the sharing of information from LSAs.

From the topological database, each router constructs a *shortest-path tree*, with itself as the root. The shortest-path tree gives the optimal route to each destination in the AS. Routing information from outside the AS appears on the tree as leaves.

OSPF routes IP traffic based solely on the destination IP address and subnet mask contained in the IP packet header.

Benefits

Benefits in large networks OSPF offers the following benefits:

- Fast convergence

  In the event of topological changes, OSPF recalculates routes quickly.

- Minimal routing protocol traffic

  Unlike distance vector routing protocols such as RIP, OSPF generates a minimum of routing protocol traffic.

- Load sharing

  OSPF provides support for equal-cost multipath routing. If several equal-cost routes to a destination exist, traffic is distributed equally among them.

- Because OSPF does not use hop count in its calculation, the routing domain is scalable.

OSPF routing algorithm

A separate copy of the OSPF routing algorithm runs in each area. Routers which are connected to multiple areas run multiple copies of the algorithm. The sequence of processes governed by the routing algorithm is as follows:

1. When a router starts, it initializes the OSPF data structures and then waits for indications from lower-level protocols that its interfaces are functional.
2. A router then uses the Hello Protocol to discover neighbors. On point-to-point and broadcast networks the router dynamically detects its neighbors by sending hello packets to the multicast address AllSPFRouters. On non-broadcast multiaccess networks, some configuration information is required in order to discover neighbors.
3. On all multiaccess networks (broadcast or non-broadcast), the Hello Protocol also elects a DR for the network.
4. The router attempts to form adjacencies with some of its neighbors. On multiaccess networks, the DR determines which routers become adjacent. This behavior does not occur if a router is configured as a passive interface, because passive interfaces do not form adjacencies.
5. Adjacent neighbors synchronize their topological databases.
6. The router periodically advertises its link-state, and also does so when its local state changes. LSAs include information about adjacencies enabling quick detection of dead routers on the network.
7. LSAs are flooded throughout the area, ensuring that all routers in an area have exactly the same topological database.

8. From this database each router calculates a shortest-path tree, with itself as root. This shortest-path tree in turn yields a routing table for the protocol.

OSPF router types

Routers in an OSPF network can take on different roles depending their configuration. The following table describes the router types in an OSPF network.

OSPF router types

Router Type	Description
Autonomous System Boundary Router (ASBR)	A router attached at the edge of an OSPF network is called an AS boundary router (ASBR). An ASBR generally has one or more interfaces that run an inter-domain routing protocol. In addition, any router distributing static routes or RIP routes into OSPF is considered an ASBR. The ASBR forwards external routes into the OSPF domain. In this way, routers inside the OSPF network learn about destinations outside their domain.
Area Border Router (ABR)	A router attached to two or more areas inside an OSPF network is considered an area border router (ABR). ABRs play an important role in OSPF networks by condensing the amount of OSPF information that is disseminated.
Internal Router (IR)	A router that has interfaces only within a single area inside an OSPF network is considered an internal router (IR). Unlike ABRs, IRs have topological information only about the area in which they are contained.
Designated Router (DR)	In a broadcast network a single router is elected to be the designated router (DR) for that network. A DR assumes the responsibility of making sure all routers on the network are synchronized with one another and also advertises that network to the rest of the AS.
Backup Designated Router (BDR)	A backup designated router (BDR) is elected in addition to the designated router (DR) and, in the event of failure of the DR, will assume its role quickly.

OSPF host route

An OSPF router with hosts directly attached to its interfaces can use host routes to advertise the attached hosts to its neighbors. You can configure up to 32 host routes.

Host routes are managed with Nortel Networks Command Line Interface (NNCLI) commands and SNMP MIBs and are identified by the host IP address and the configured route type of service (TOS). For each host directly connected to the router, configure the cost of the link to the host during host creation. You cannot modify this cost.

Note: Always set TOS to 0 because TOS-based routing is not supported.

When a host is added to, or deleted from, a host route, the router updates the router LSAs and floods them to neighbors in each area where that router has an interface.

Following is an example of parameters for a host route advertised in the LSA.

Host route in LSA

- Type: 3 (stub network)
- LinkID: IP address of host directly connected to router
- Link Data: 0xFFFFFFFF
- Metric: configured cost of host

OSPF Enhancements

- Host route - Allows a router to advertise to its neighbors all hosts that are directly attached to that router's interfaces. Up to 32 host routes can be configured.
- Virtual links - The OSPF network can be partitioned into multiple areas. However, a backbone area must exist and be contiguous, and every non-backbone area must be connected to the backbone area using either a physical or a logical link. In a network where a physical connection between the non-backbone area and backbone area is impossible, use of a virtual link provides the logical connection through another non-backbone area, called the transit area. Virtual links can be created manually or automatically. The 5500 Series switch supports up to 16 virtual links.

When 5500 Series switches are stacked, and a unit leaves the stack and becomes standalone, the router ID is automatically changed to its default value if IP blocking is turned off and OSPF is globally enabled. This prevents duplication of a router ID in the OSPF routing domain. The new router ID value is temporary, that is, it is not saved to NVRAM. Therefore, upon reset, the old router ID is restored. Configurable using NNCLI, ACG, and Device Manager.

Example configurations The following is an example for creating a host route:

Creating Host Route

Example : 1

```
R3(config)#router ospf
R3(config-router)#host-route 11.11.11.111 metric 10
R3(config-router)#show ip ospf host-route
```

Host IP	Metric
11.11.11.111	10

```
R3(config-router)#
```

The following is an example for deleting a host route:

Deleting Host Route

Example : 1

```
R3(config-router)#no host-route 11.11.11.111
R3(config-router)#show ip ospf host-route
```

Host IP	Metric

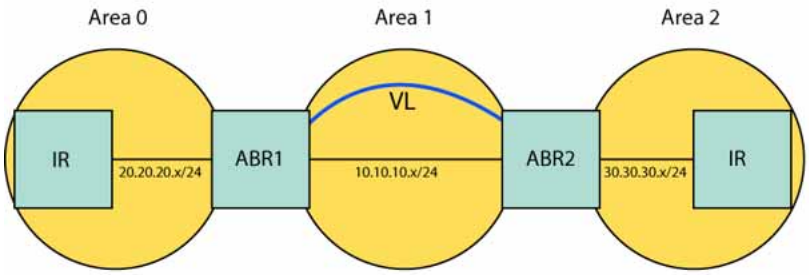
```
R3(config-router)#
```

OSPF virtual link

On an OSPF network, a router acting as an area boundary router (ABR) must be directly connected to the backbone. If no physical connection is available, you can create a virtual link.

A virtual link is established between two endpoint ABRs and is a logical connection to the backbone area through a non-backbone area called a transit area. In the following diagram, non-backbone ABR 2 establishes a virtual link with backbone ABR1 across transition area, area 1. The virtual link connects area 2 to area 0.

Virtual link diagram



Note: Stub or NSSA areas cannot be transit areas.

A virtual link can be created manually or automatically.

Manual virtual link creation can conserve resources and provide specific control of virtual link placement in the OSPF configuration.

To add a virtual link manually, configure both endpoint ABRs with a neighbor router ID and transit area ID. You can configure up to 16 virtual links.

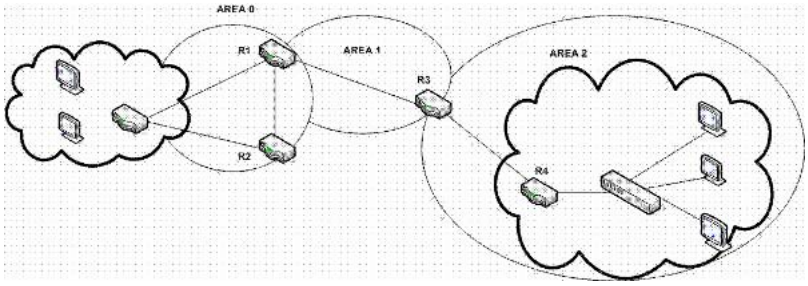
Note: You can modify parameters for manually added virtual links.

To accept automatic virtual link creation, enable automatic virtual link on both endpoint ABRs (the default value is disabled). Automatic virtual links are removed when the transit area is deleted, auto virtual link is disabled, or the router is no longer an ABR.

Note: Auto-created virtual links use default settings that cannot be modified.

Example Configuration

Consider the following situation:



In this case, R4 in Area2 cannot be physically connected to Area0 (for some reason) and it will be connected to R3 which is NOT a backbone ABR (like R1 is for instance). As Area2 is not directly connected to backbone Area0 or directly connected to a backbone ABR router, clients from Area2 will not be able to access anything outside Area2. Also, router R3 is an ABR router connected to two non-backbone areas.

In order to solve these problems, virtual-link must be configured between router R3 and R1 which are both ABRs. Virtual-link cannot be configured on non-ABR routers.

Consider the following Router IDs:

- R1 : 1.0.0.0
- R3 : 3.0.1.0
- R4 : 4.0.2.0

Virtual-link can be configured in two ways on ABR routers :

- Configuring virtual link manually
- Configuring virtual link automatically

The following is an example for creating an auto virtual link:

Creating auto virtual link

```
R1 (config-router)#auto-vlink
```

Example : 1

```
R1(config)#show ip ospf
Router ID:  1.0.0.0
Admin Status:  Enabled
Version Number:  2
Area Border Router Oper Status:  True
AS Boundary Router Config Status:  False
External Link-State Advertisements:  0
External Link-State Checksum:  0(0x0)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  67
New Link-State Advertisements Received:  722
```

```
   OSPF Traps:  Disabled
   Auto Virtual Link Creation:  Enabled
   SPF Hold-Down Time:  10
   RFC 1583 Compatibility:  Enabled

   R3 (config-router)#auto-vlink

   Example : 2
   R3(config)#show ip ospf
   Router ID:  3.0.1.0
   Admin Status:  Enabled
   Version Number:  2
   Area Border Router Oper Status:  True
   AS Boundary Router Config Status:  False
   External Link-State Advertisements:  0
   External Link-State Checksum:  0(0x0)
   Type-of-Service (TOS) Routing Supported:  False
   Originated Link-State Advertisements:  67
   New Link-State Advertisements Received:  722
   OSPF Traps:  Disabled
   Auto Virtual Link Creation:  Enabled
   SPF Hold-Down Time:  10
   RFC 1583 Compatibility:  Enabled
```

The following is an example for deleting an auto virtual link:

Deleting auto virtual link

```
R1 (config-router)#no auto-vlink

   Example : 1
   R1(config)#show ip ospf
   Router ID:  1.0.0.0
   Admin Status:  Enabled
   Version Number:  2
   Area Border Router Oper Status:  True
   AS Boundary Router Config Status:  False
   External Link-State Advertisements:  0
   External Link-State Checksum:  0(0x0)
   Type-of-Service (TOS) Routing Supported:  False
   Originated Link-State Advertisements:  67
   New Link-State Advertisements Received:  722
   OSPF Traps:  Disabled
   Auto Virtual Link Creation:  Disabled
   SPF Hold-Down Time:  10
   RFC 1583 Compatibility:  Enabled

R3 (config-router)#no auto-vlink

   Example : 2
   R3(config)#show ip ospf
```

```
Router ID:  3.0.1.0
Admin Status:  Enabled
Version Number:  2
Area Border Router Oper Status:  True
AS Boundary Router Config Status:  False
External Link-State Advertisements:  0
External Link-State Checksum:  0(0x0)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  67
New Link-State Advertisements Received:  722
OSPF Traps:  Disabled
Auto Virtual Link Creation:  Disabled
SPF Hold-Down Time:  10
RFC 1583 Compatibility:  Enabled
```

Virtual-Link can also be configured using the Java Device Manager (JDM). Just go under IP Routing > OSPF menu. There you can find : ‘General’ tab for Auto-Vlink creation, ‘Virtual If’ tab, and ‘Virtual Neighbors’ tab.

Route policies

Route policies are a Nortel proprietary improvement on existing routing schemes. Using existing routing schemes, packets are forwarded based on routes that have been learned by the router through routing protocols such as RIP and OSPF or through the introduction of static routes. Route policies introduce the ability to forward packets based on rule sets created by the network administrator. These rule sets, or policies, are then applied to the learned or static routes.

Route policies on the Nortel Ethernet Routing Switch 5500 Series supports the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) protocol. When used in conjunction with these protocols, route policies can be used to perform the following tasks that are not possible using traditional routing methods:

- Listen for routing updates from specific gateways.
- Listen for routing updates from specific networks.
- Assign a specific subnet mask to be included with a network in the routing table.
- Advertise routing updates from specific gateways.
- Advertise routing updates to specific networks.
- Assign a specific subnet mask to be included in the route summary packets.
- Advertise routes learned by one protocol to another.

Route policies supports the following types of policies:

- **Accept (In) Policies**

  Accept polices are applied to incoming routing updates before they are applied to the routing table. In the case of RIP, accept policies can be applied to all incoming packets and only one policy can be created for each RIP interface. In the case of OSPF, accept policies are only applied to Type 5 External routes based on the advertising router ID. There can only be one OSPF accept policy per switch and the policy is applied before updates are added to the routing table from the link state database.

- **Announce (Out) Policies**

  Announce policies are applied to outgoing routing updates before the routing update packets are actually transmitted from the switch. In the case of RIP, announce policies can be applied to all outgoing packets and only one policy can be created for each RIP interface. Announce policies are not supported for OSPF as OSPF requires routing information to be consistent throughout the OSPF domain.

- **Redistribution Policies**

  Redistribution policies are used to provide notification of addition or deletion of a route in the routing table by one protocol to another protocol. OSPF redistribution policies send redistributed routes as Type 5 External routes. There can be only one OSPF redistribution route per switch and it must be configured as a ASBR with redistribution enabled.

Route policies consist of the following items:

- **Prefix Lists**
  - List of IP addresses with subnet masks.
  - Identified by a prefix list name and unique identifier.
  - Prefix lists support the comparison of ranges of incoming masks.
- **Route Maps**
  - Contain a set of match and set parameters.
  - Match and set parameters can contain several prefix lists.
  - A set of match and set parameters are identified by a sequence number.
  - Accept and deny actions are associated with each sequenced parameter set.
  - Sequence numbers act as a preference setting. Sets with a lower sequence number are preferred over those with a higher sequence number.

To configure routing policies, create the appropriate prefix lists and then assign those prefix lists to route maps. Once all route maps have been created, assign them to the appropriate type of policy.

In a stacked environment, the following rules are applied to routing policies:

- The policy database is stored in all stack units.
- Policy configuration is supported from only the base unit. The base unit sends updates to non-base units to update the policy database in each stack unit.
- During database updates, only the database in the base unit is synchronized with the non-base unit. The database in the non-base units are deleted during the exchange.
- Only the policies stored in the base unit are used by RIP and OSPF for policy application.

Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure that can occur when the single static default gateway router for an end station is lost. VRRP introduces the concept of a virtual IP address (transparent to users) shared between two or more routers connecting a common subnet to the enterprise network. With the virtual IP address as the default gateway on end hosts, VRRP provides dynamic default gateway redundancy in the event of failure.

VRRP uses the following terms:

- **VRRP router** - a router running the VRRP protocol.
- **Virtual router** - the abstract object managed by VRRP that is assigned the virtual IP address and that acts as the default router for a set of IP addresses across a common network. Each virtual router is assigned a virtual router ID.
- **Virtual router master** - the VRRP router that assumes responsibility for forwarding packets sent to the IP address associated with the virtual router. The master router also responds to packets sent to the virtual router IP address and answers ARP requests for this IP address.
- **Virtual router backup** - the router or routers that can serve as the failover router if the master router becomes unavailable. If the master router fails, an election process provides a dynamic transition of forwarding responsibility to a new master router.
- **Priority** - an 8-bit value assigned to all VRRP routers. A higher value represents a higher priority for election to the master router. The priority can be a value from 1 to 255. When a master router fails, an election process takes place among the backup routers to dynamically reassign the role of the master router.

Equal Cost MultiPath (ECMP)

The Equal Cost MultiPath (ECMP) feature allows routers to determine equal cost paths to the same destination prefix. The multiple paths can be used for load sharing of traffic and allows faster convergence to other active paths in case of network failure. By maximizing load sharing among equal-cost paths, links between routers can be used more efficiently when sending IP traffic. The ECMP feature supports and complements the following protocols types:

- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP)
- Static Routes

ECMP is only supported on the Nortel Ethernet Routing Switch 5520 and 5530. ECMP will work in a mixed stack but will not run on any Nortel Ethernet Routing Switch 5510 units in the stack.

UDP broadcast forwarding

Some network applications, such as the NetBIOS name service, rely on User Datagram Protocol (UDP) broadcasts to request a service or locate a application. If a host is on a network, subnet segment, or VLAN that includes a server for the service, UDP broadcasts are by default not forwarded to the server located on a different network segment or VLAN. This is resolved by forwarding the broadcasts to the server through physical or virtual interfaces.

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address. The packet is sent as a unicast packet to the server.

The following are the basic steps for UDP broadcast forwarding configuration:

1. Enter the UDP protocols to be forwarded.
2. Create forwarding policies by defining UDP protocol and server pairs.
3. Assemble these policies into lists.
4. Apply these lists to the appropriate interfaces.

When a UDP broadcast is received on a router interface, it must meet the following criteria if it is to be considered for forwarding:

- It must be a MAC-level broadcast.
- It must be an IP-limited broadcast.
- It must be for a configured UDP protocol.
- It must have a TTL value of at least 2.

For each ingress interface and protocol, the UDP broadcast packets are forwarded only to a unicast host address (the unicast IP address of the server for example).

Dynamic Host Configuration Protocol (DHCP) / Bootstrap Protocol (BootP)

DHCP-BootP relay

The Dynamic Host Configuration Protocol (DHCP) is an extension of the Bootstrap protocol (BootP) and provides host configuration information to workstations on a dynamic basis. To lower administrative overhead, network managers prefer to configure a small number of DHCP servers in a central location. It is necessary for routers to support the BootP/DHCP relay function so that hosts can access configuration information from servers several router hops away.

Differences between DHCP and BootP

The following differences between DHCP and BootP are specified in RFC 2131 and include functions that BootP does not address:

- The Nortel Ethernet Routing Switch 5500 Series supports the Bootstrap protocol (BootP). BootP enables the retrieval of an ASCII configuration file name and configuration server address.
- A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask and the IP address of the default router (default gateway).
- DHCP defines mechanisms through which clients can be assigned a network address for a finite lease (allowing for reuse of IP addresses).
- DHCP provides the mechanism for clients to acquire all of the IP configuration parameters needed to operate.

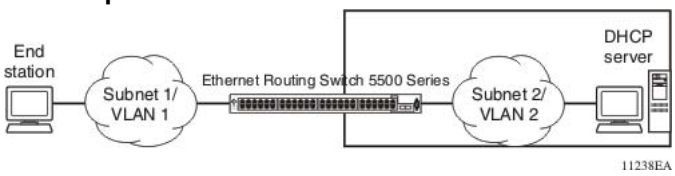
DHCP uses the BootP message format defined in RFC 951. The remainder of the options field consists of a list of tagged parameters that are called "options" (RFC 2131).

Summary of DHCP relay operation

BootP/DHCP clients (workstations) generally use UDP/IP broadcasts to determine their IP addresses and configuration information. If such a host is on a network or a subnet segment (or VLAN) that does not include a DHCP server, the UDP broadcasts are by default not forwarded to the server located on a different network segment or VLAN. The Nortel Ethernet Routing Switch 5500 Series can be configured to resolve this issue by forwarding the broadcasts to the server. The router interfaces can be configured to forward DHCP broadcasts to other locally connected network segments or directly to the server’s IP address. DHCP must be enabled on a per-VLAN basis.

"DHCP operation" (page 40)Figure DHCP operation shows an end station connected to subnet 1, corresponding to VLAN 1. The Nortel Ethernet Routing Switch 5500 Series connects two subnets by means of the virtual routing function. When the end station generates a DHCP request as a limited UDP broadcast to the IP address of all 1s (that is, 255.255.255.255) with the DHCP relay function configured, the Nortel Ethernet Routing Switch 5500 Series forwards DHCP requests to subnet 2 or to the host address of the DHCP server, depending on the configuration.

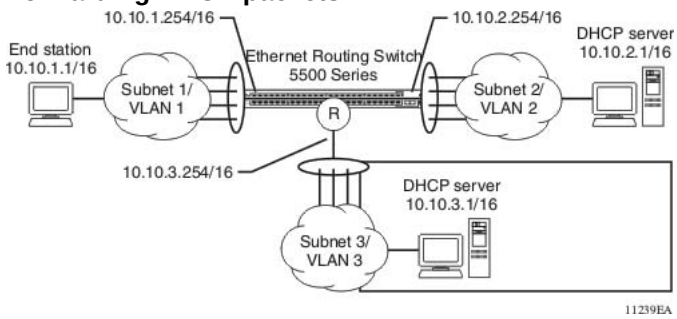
DHCP operation



Forwarding DHCP packets

In the example shown in "Forwarding DHCP packets" (page 40), the agent address is 10.10.1.254. To configure the Nortel Ethernet Routing Switch 5500 Series to forward DHCP packets from the end station to the server, use 10.10.2.1 as the server address.

Forwarding DHCP packets



All BootP broadcast packets, including DHCP packets that appear on the VLAN 1 router interface (10.10.1.254), will be forwarded to the DHCP server. In this case, the DHCP packets are forwarded as unicast to the DHCP server's IP address.

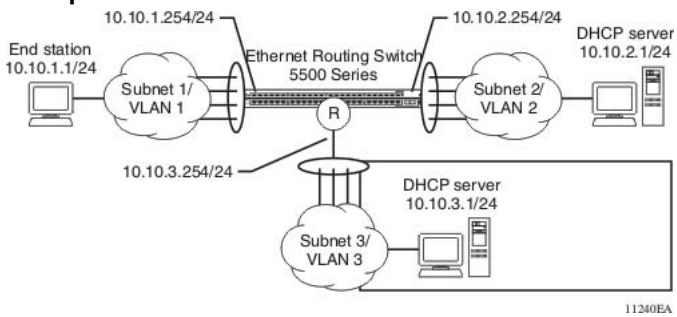
Multiple BootP-DHCP servers

Most enterprise networks use multiple BootP/DHCP servers for fault tolerance. The Nortel Ethernet Routing Switch 5500 Series allows switch configuration to forward BootP/DHCP requests to multiple servers. Up to 10 servers can be configured to receive copies of the forwarded BootP/DHCP messages.

If a DHCP client is connected to a routable interface, to configure DHCP requests to be sent to up to 512 different routable interfaces or 512 different server IP addresses, enable DHCP on the client (agent address) and then enable DHCP from the client to each of the interfaces or IP addresses (server addresses).

In the example shown in "Multiple BootP/DHCP servers" (page 41), two DHCP servers are located on two different subnets. To configure the Nortel Ethernet Routing Switch 5500 Series to forward the copies of the BootP/DHCP packets from the end station to both servers, specify the switch (10.10.1.254) as the agent address. Then enable DHCP to each of the DHCP servers by entering 10.10.2.1 and 10.10.3.1 as the server addresses.

Multiple BootP/DHCP servers



Setting DHCP

To set DHCP, take the following steps:

Step	Action
1	Enable IP routing on the Nortel Ethernet Routing Switch 5500 Series and on the target VLAN interface.
2	Enable DHCP globally. ***Note:*** DHCP is enabled by default.
3	Set the DHCP forwarding paths, using the VLAN IP as the starting point, or agent IP.
4	Set the mode for each DHCP forwarding path.
5	Enable DHCP for the specific VLAN.
6	Enable the DHCP broadcast message for the specific VLAN.

—End—

Any of the Nortel Ethernet Routing Switch 5500 Series switch management systems can be used to set DHCP.

DHCP relay

DHCP (Dynamic Host Configuration Protocol) is a mechanism to assign network IP addresses to clients who request an address. It is built on top of the existing BOOTP protocol and can be specified for DHCP, BOOTP, or both.

The DHCP relay feature relays client requests to DHCP servers on different L3 VLANs. It also relays server replies back to the clients.

DHCP relay can be configured through Command Line Interface or Java Device Manager. DHCP can only be configured on the base unit from CLI, like all L3 commands. There are three parts in the DHCP relay configurations. They are:

- global DHCP enable/disable
- interface configurations
- forward path configurations

To relay DHCP messages, two VLANs must be created and IP addresses assigned to them. The client and server must reside on different L3 VLANS to use DHCP relay. IP routing and global DHCP relay must be enabled on both the client as well as server.

> ***Note:*** The DHCP Relay feature shares resources with QoS. If the DHCP Relay feature is enabled, a QoS policy with a precedence of 11 cannot be installed.
>
> For further information on QoS policies refer to *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service* (Part Number NN47200-504).

Global DHCP relay configuration This configuration enables or disables DHCP relay for the entire unit or stack. Once DHCP relay is disabled, the switch/stack will not relay DHCP/BOOTP " Global DHCP relay commands" (page 42)across L3 VLANs. However, the settings will still be configurable.

describes the global DHCP relay commands.

Global DHCP relay commands

Command	Description
show ip dhcp-relay	shows global DHCP relay state
no ip dhcp-relay	disables DHCP relay globally
ip dhcp-relay	enables DHCP relay globally

These commands must be executed in the Global Configuration command mode.

Interface DHCP relay configurations These configurations are associated with the L3 VLAN that the client or server resides on. IP routing must be enabled and a valid IP address must be assigned to the L3 VLAN before it generates the default settings for DHCP relay.

"Interface DHCP relay commands" (page 43)describes the interface DHCP relay commands. To change the interface DHCP relay configurations, switch to the Interface Configuration command mode.

Interface DHCP relay commands

Command	Description
show vlan dhcp-relay	shows vlan dhcp relay state
ip dhcp-relay min-sec 30	sets min-sec to 30
ip dhcp-relay mode dhcp	sets mode to dhcp
no ip dhcp-relay	disables ip dhcp-relay
ip dhcp-relay broadcast	enables broadcast for this interface

DHCP Relay forward path configurations These configurations are made per interface IP address and server IP address. " DHCP relay forward path commands" (page 43)DHCP relay forward path commands table describes the ip dhcp relay fwd-path commands.

DHCP relay forward path commands

Command	Description
show ip dhcp-relay fwd-path	Shows ip dhcp-relay fwd-path.
ip dhcp-relay fwd-path <agent IP> <server IP> mode bootp-dhcp	Creates interface IP and server IP path with modes DHCP & BootP.
ip dhcp-relay fwd-path <agent IP> <server IP> disable	Disables the interface/server pair, enable = false.
no dhcp-relay fwd-path <agent IP> <server IP>	Deletes the interface/server pair.
no ip dhcp-relay	Disables ip dhcp-relay.
ip dhcp-relay broadcast	Enables broadcast for this interface.

DHCP relay uses a hardware resource that is shared by switch Quality of Service applications. When DHCP relay is enabled globally, the Quality of Service filter manager will not be able to use precedence 11 for configurations. For the filter manager to be able to use this resource, DHCP relay must be disabled for the entire unit or stack.

Avoiding duplicate IP addresses

The Nortel Ethernet Routing Switch 5500 Series has built-in safeguards to avoid issuing duplicate IP addresses, because the switch functions as a stack as well as a stand-alone system. These safeguards apply to stack configuration changes (for example, when a stack is forming or after a unit is removed from a stack).

The system allows the use of an existing IP address under the following conditions:

- When a unit leaves a stack:
  - If the unit was the acting Base Unit (BU) of the stack and the stack consisted of only two units.
  - If the IP blocking mode in the stack was set to none.
- When a unit boots up:
  - If the unit was never in a stack.
  - If IP blocking was manually turned off prior to the current boot.
  - If the unit was the designated Base Unit (BU); that is, selected by hardware switch on the unit, either on the back or on the UI button on the front; and the stack consisted of only two units.
  - If the IP blocking mode was set to none.

If the desired switch IP address is blocked by the system, then the address must be configured manually in the command line interface.

Automatic router ID change

If a unit leaves the stack and becomes standalone (when the stack disjoins), the router ID is automatically changed to its default value. This prevents router ID duplication in the OSPF routing domain.

Prerequisites: IP blocking must be turned off (set to none) and OSPF must be globally enabled.

TIP: The change in router ID is temporary (not saved in non-volatile random access memory) and, upon reset, the router ID is restored.

IP blocking

IP Blocking is a Layer 3 feature of the Nortel Ethernet Routing Switch 5500 Series that provides built-in safeguards for the usage of duplicate IP addresses in a stacked environment. IP Blocking is used whenever a unit leaves a stack or is rebooting inside the context of a stack. Depending on the setting in use, Layer 3 functionality is either continued or blocked by this feature.

IP Blocking can exist in either a *none* or *full* condition. When IP Blocking is set to *none*, duplicate IP addresses are permitted in the stack unconditionally. When the *full* condition is set, duplicate IP addresses are blocked in the stack unconditionally.

In a stack environment, Nortel recommends that IP blocking mode *none* be used in a stack of 2 units. In such a stack environment and IP blocking mode combination, the following functional characteristics can be expected:

- If the stack base unit becomes non-operational the following will occur:
  - Layer 3 functionality will continue to run on the non-base unit.
  - Dynamic routing protocols still run on the non-base unit.
- If the stack non-base unit becomes non-operational the following will occur:
  - Layer 3 functionality will continue to run on the base unit.
  - Dynamic routing protocols run on the base unit.

A disadvantage of this configuration is that if the non-operational unit does not rejoin the stack, address duplication will occur.

In stack environments of more than 2 units, Nortel recommends using IP blocking mode *full*. In such a stack environment and IP blocking mode combination, the following functional characteristics can be expected:

- If the stack base unit becomes non-operational the following will occur:
  - The temporary base unit takes over base unit duties.
  - The temporary base unit runs the Layer 3 and DRP functionality.
  - The takeover of the temporary base unit will cause the MAC addresses of the Layer 3 interfaces to change and the MAC addresses from the temporary base unit MAC address pool are used. This may cause a minor disruption in routing traffic. To facilitate quick failover in this instance, gratuitous ARP messages are sent out for each interface for 5 minutes at 15 second intervals.
- If a stack non-base unit becomes non-operational the following will occur:

— The stack will continue to run normally with the base unit controlling Layer 3 and DRP functionality.

— If the non-operational non-base unit does not rejoin the stack, no Layer 3 or DRP functionality will run on it.

IGMP snooping

The Nortel Ethernet Routing Switch 5500 Series can sense Internet Group Management Protocol (IGMP) host membership reports from attached stations and use this information to set up a dedicated path between the requesting station and a local IP Multicast router. After the pathway is established, the Nortel Ethernet Routing Switch 5500 Series switch blocks the IP Multicast stream from exiting any other port that does not connect to another host member, thus conserving bandwidth. The following section describes how Nortel Ethernet Routing Switch 5500 Series switches provide the same benefit as IP Multicast routers, but in the local area.

IGMP is used by IP Multicast routers to learn about the existence of host group members on their directly attached subnets (see RFC 2236). The IP Multicast routers get this information by broadcasting IGMP queries and listening for IP hosts reporting their host group memberships. This process is used to set up a client/server relationship between an IP Multicast source that provides the data streams and the clients that want to receive the data.

By default, unknown multicast traffic is flooded to all ports in a VLAN. In situations in which there is a multicast transmitter that is not doing IGMP and there are no multicast receivers, the traffic transmitted by the transmitter is flooded.

The CLI commands for IGMP allow the sending of all unknown multicast traffic to IGMP static router ports only. This traffic will not be forwarded to dynamically discovered m-router ports. If it is desirable to forward unknown unicast traffic to certain ports only, those ports can be set as static m-router ports.

- When disabled, the Nortel Ethernet Routing Switch 5500 Series switch treats unknown multicast traffic as it does broadcast traffic (flood). This is the default behavior.
- User settings for the Unknown Multicast No Flood feature is stored in NVRAM. In a stack, if settings on different units differ, the Base Unit setting will take precedence. This feature can be enabled or disabled at any time.
- Nortel Networks recommends this feature be enabled when IGMP snooping is enabled.

"IP multicast propagation with IGMP routing" (page 47)shows how IGMP is used to set up the path between the client and server. As shown in this example, the IGMP host provides an IP Multicast stream to designated routers that forward the IP Multicast stream on their local network only if there is a recipient.

The client/server path is set up as follows:

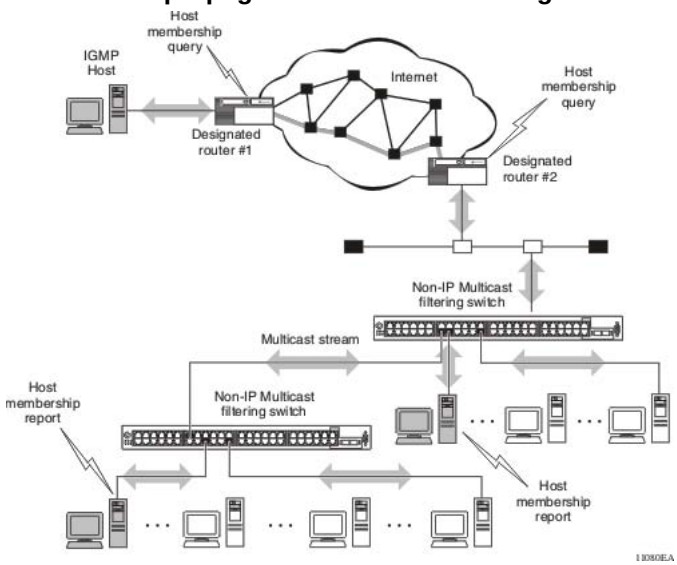
1. The designated router sends out a host membership query to the subnet and receives host membership reports from end stations on the subnet.
2. The designated routers then set up a path between the IP Multicast stream source and the end stations.
3. Periodically, the router continues to query end stations about whether to continue participation.
4. As long as any client continues to participate, all clients, including non-participating end stations on that subnet, receive the IP Multicast stream.

   Note: Although the non-participating end stations can filter the IP Multicast traffic, the IP Multicast traffic still exists on the subnet and consumes bandwidth.

IP Multicast can be optimized in a LAN by using IP Multicast filtering switches, such as the Nortel Ethernet Routing Switch 5500 Series.

As shown in "IP multicast propagation with IGMP routing" (page 47), a non-IP Multicast filtering switch causes IP Multicast traffic to be sent to all segments on the local subnet.

IP multicast propagation with IGMP routing

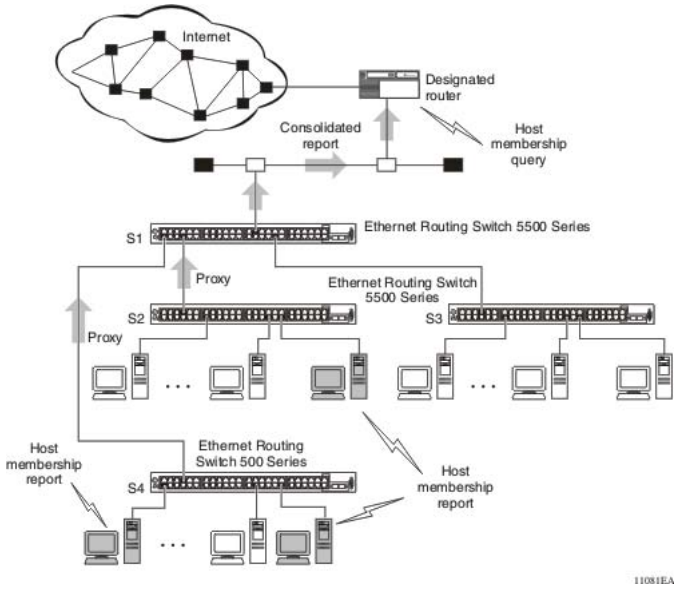


The Nortel Ethernet Routing Switch 5500 Series can automatically set up IP Multicast filters so the IP Multicast traffic is only directed to the participating end nodes (see).

In , "5500 Series switch filtering IP multicast streams (1 of 2)" (page 48)switches S1 to S4 represent a LAN connected to an IP Multicast router. The router periodically sends Host Membership Queries to the LAN and listens for a response from end stations. All of the clients connected to switches S1 to S4 are aware of the queries from the router.

One client, connected to S2, responds with a host membership report. Switch S2 intercepts the report from that port, and generates a proxy report to its upstream neighbor, S1. Also, two clients connected to S4 respond with host membership reports, causing S4 to intercept the reports and to generate a consolidated proxy report to its upstream neighbor, S1.

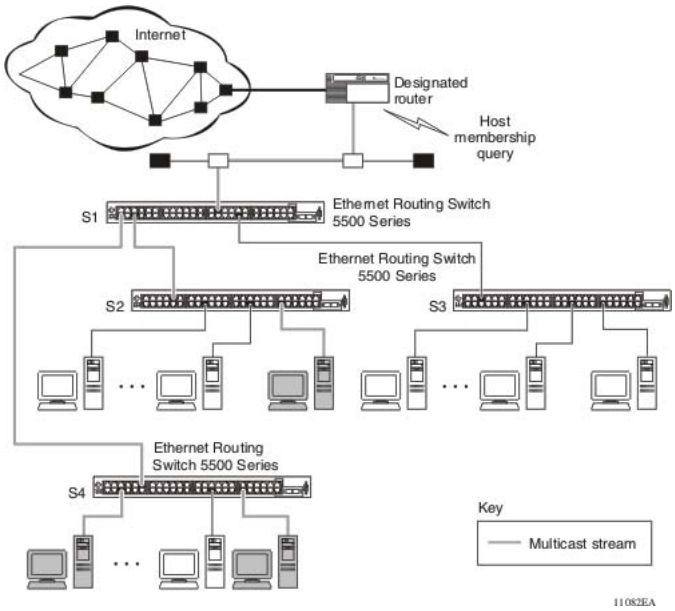
5500 Series switch filtering IP multicast streams (1 of 2)



Switch S1 treats the consolidated proxy reports from S2 and S4 as if they were reports from any client connected to its ports, and generates a consolidated proxy report to the designated router. In this way, the router receives a single consolidated report from that entire subnet.

After the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast ("5500 Series switch filtering IP multicast streams (2 of 2)" (page 49)).

5500 Series switch filtering IP multicast streams (2 of 2)



The consolidated proxy report generated by the switch remains transparent to Layer 3 of the International Standardization Organization, Open Systems Interconnection (ISO/OSI) model. (The switch IP address and MAC address are not part of proxy report generation.) The last reporting IGMP group member in each VLAN represents all of the hosts in that VLAN and IGMP group.

IGMP snooping configuration rules

The IGMP snooping feature operates according to specific configuration rules. When configuring the switch for IGMP snooping, consider the following rules that determine how the configuration reacts in any network topology:

- There is a maximum of 240 groups on the Nortel Ethernet Routing Switch 5500 Series.
- A port that is configured for port mirroring cannot be configured as a static router port.
- If a MultiLink Trunk member is configured as a static router port, all of the MultiLink trunk members are configured as static router ports. Also, if a static router port is removed, and it is a MultiLink Trunk member, all MultiLink trunk members are removed as static router port members, automatically.
- Static router ports must be port members of at least one VLAN.
- The IGMP snooping feature is not STP dependent.
- The IGMP snooping feature is not Rate Limiting dependent.

- The snooping field must be enabled for the proxy field to have any valid meaning.
- Static router ports are configured per VLAN and per IGMP Version.

Note: Because IGMP snooping is set up per VLAN, all IGMP changes are implemented according to the VLAN configuration for the specified ports.

IP Routing Configuration and Management

This chapter describes the configuration and management of IP routing in the Nortel Ethernet Routing Switch 5500 Series. IP Routing configuration is accomplished through the Command Line Interface (CLI), Web-based Management Interface, or the Java Device Manager (JDM).

This chapter contains the following topics:

IP routing initial configuration

This section provides step by step instructions for the initial configuration of the IP routing protocols supported by the Nortel Ethernet Routing Switch 5500 Series. For conceptual information about IP routing topics covered in this section, refer to "An Introduction to IP Routing Protocols" (page 13). This section contains the following topics:

This chapter also contains in-depth configuration examples that can aid in the advanced configuration of the switch. Refer to "IP routing configuration examples" (page 120)for these advanced examples.

Global IP routing configuration

Before IP routing configuration can take place, IP routing must be globally enabled on the switch. Use the set of commands outlined below to enter the Global Configuration mode of the switch and enable IP routing.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# ip routing
```

Open Shortest Path First (OSPF) initial configuration

This section contains the steps necessary for the initial configuration of OSPF on the switch. More advanced configuration examples can be found in the "IP routing configuration examples" (page 120)section.

Basic OSPF configuration

A basic OSPF configuration will learn OSPF routes from other OSPF devices and propagate routes to other OSPF devices. The following procedure outlines the creation of a basic OSPF configuration:

Step	Action
1	Log into User EXEC mode. `5530-24TFD> enable`

2	Log into Global Configuration mode.
	`5530-24TFD# config terminal`
	The switch will respond with the following line:
	`Enter configuration commands, one per line. End with CNTL/Z.`

3	Enable IP routing globally. `5530-24TFD(config)# ip routing`
4	Enable OSPF globally. `5530-24TFD(config)# router ospf en`
5	Log into the OSPF router configuration mode. It is not necessary to make any changes at this time but entering the router configuration mode is a good way to verify that the mode has been activated. `5530-24TFD(config)# router ospf` ***Note:*** The remainder of this procedure refers to VLAN 35. Although VLAN 35 is used for this example, any port type VLAN could be used.
6	Create a port type VLAN as VLAN number 35 in spanning tree protocol group 1. `5530-24TFD(config)# vlan create 35 type port 1`
7	Log into the Interface Configuration mode for VLAN 35. `5530-24TFD(config)# interface vlan 35`
8	Enable IP routing on VLAN 35. `5530-24TFD(config-if)# ip routing`

9 Assign an IP address to VLAN 35.

```
5530-24TFD(config-if)# ip address 1.1.2.25
255.255.255.0
```

10 Enable OSPF in VLAN 35.

```
5530-24TFD(config-if)# ip ospf en
```

11 Return to Global Configuration mode.

```
5530-24TFD(config-if)# exit
```

12 By default all ports belong to a newly created VLAN. This command removes all of the ports from VLAN 35 .

```
5530-24TFD(config)# vlan members remove 35 all
```

13 Add ports 1 through 10 to VLAN 35.

```
5530-24TFD(config)# vlan members add 35 1-10
```

—End—

Basic ASBR configuration

The Autonomous System Boundary Router (ASBR) is used in OSPF to import routes that come from non-OSPF sources such as:

- Local interfaces that are not part of OSPF.
- RIP interfaces.
- RIP learned routes.
- Static routes.

This quick reference will help in the configuration of OSPF to import these types of routes. This will allow the rest of the OSPF network to learn them as OSPF routes. To create a basic ASBR configuration, follow this procedure:

Step	Action

1 Log into User EXEC mode.

```
5530-24TFD> enable
```

2 Log into Global Configuration mode.

```
5530-24TFD# config terminal
```

The switch will respond with the following line:

```
Enter configuration commands, one per line.  End with
CNTL/Z.
```

3 Log into the OSPF router configuration mode.

```
5530-24TFD(config)# router ospf
```

4 Enable ASBR functionality.

```
5530-24TFD(config-router)# as-boundary-router en
```

5 Use the following commands to select the type of routes that OSPF will distribute to other OSPF devices. RIP, direct, and static routes are supported.

```
5530-24TFD(config-router)# redistribute rip en
5530-24TFD(config-router)# redistribute direct en
5530-24TFD(config-router)# redistribute static en
```

6 Return to Global Configuration mode.

```
5530-24TFD(config-router)# exit
```

7 Once the commands in step 5 have be used to select the types of routes to redistribute, apply the changes globally with the following commands.

```
5530-24TFD(config)#ip ospf apply redistribute rip
5530-24TFD(config)#ip ospf apply redistribute direct
5530-24TFD(config)#ip ospf apply redistribute static
```

—End—

Configuring ECMP for OSPF

Usage of ECMP with OSPF is supported on the 5520 and 5530 models only. To configure ECMP with OSPF, use the following procedure:

Step	Action

1 Log into User EXEC mode.

```
5530-24TFD> enable
```

2 Log into Global Configuration mode.

```
5530-24TFD# config terminal
```

The switch will respond with the following line:

```
Enter configuration commands, one per line.  End with
CNTL/Z.
```

3 Set the number of ECMP paths to use with OSPF. Up to four paths can be used.

```
5530-24TFD(config)# ospf maximum-path 2
```

This command tells the router to use up to two paths to get to any OSPF network destination.

4 The configuration can be verified using the following command.

```
5530-24TFD(config)# show ecmp
```

—End—

IP routing configuration using the CLI

This section describes the various Command Line Interface commands available for the configuration and management of IP routing. Depending on the type of command and the context in which it is being used, these commands are executed in the various CLI command modes.

IP configuration commands

This section describes the commands for the global IP configuration at the switch level.

ip routing command

The **ip routing** command enables global routing at the switch level.

The syntax for the **ip routing** command is:

```
ip routing
```

The **ip routing** command is executed in the Global Configuration command mode.

no ip routing command

The **no ip routing** command disables IP routing.

The syntax for the **no ip routing** command is:

```
no ip routing
```

The **no ip routing** command is executed in the Global Configuration command mode.

ip blocking-mode command

Use this command to set the level of IP blocking to perform in the stack. The syntax for this command is:

```
ip blocking-mode {full | none}
```

The following table outlines the parameters for this command.

ip blocking-mode parameters

Parameter	Description
full	Select this parameter to set IP blocking to full. This never allows a duplicate IP address in a stack.
none	Select this parameter to set IP blocking to none. This allows duplicate IP addresses unconditionally.

This command is executed in the Global Configuration command mode.

Layer 3 routable VLANs

The Nortel Ethernet Routing Switch 5500 Series are Layer 3 (L3) switches. This means that a regular L2 VLAN becomes a routable L3 VLAN if an IP address and MAC address are attached to the VLAN. When routing is enabled in L3 mode, every L3 VLAN is capable of routing as well as carrying the management traffic. The user can use any L3 VLAN instead of the Management VLAN to manage the switch.

This section covers the commands that are used to set up and configure routable VLANs.

interface vlan command

The **`interface vlan`** command only takes to the interface config mode. The **`ip routing`** command in the interface-config mode enables routing on a specific vlan.

The syntax for the **`interface VLAN`** command is:

```
interface vlan <1 - 4094>
```

The **`interface VLAN`** command is executed in the Global Configuration command mode.

ip address command

The **`ip address`** command enables routing on a VLAN.

The syntax for the **`ip address`** command is:

```
ip address  <A.B.C.D> <W.X.Y.Z>  [<1 - 256>] [secondary]
```

The **`ip address`** command is executed in the Interface Configuration command mode.

The following table describes the parameters for this command.

ip address parameters

Parameter	Description
<A.B.C.D>	The IP address to attach to the VLAN.
<W.X.Y.Z>	The subnet mask to attach to the VLAN
<1 - 256>	The MAC offset value. Specify the value 1 for the Management VLAN only.
secondary	Use this option to set up a secondary IP interface on a VLAN. You can have a maximum of eight secondary IP interfaces for every primary and the primary must be set up before any secondary interfaces are configured.

no ip address command

The **no ip address** command disables routing on a VLAN.

The syntax for the **no ip address** command is:

```
no ip address  <A.B.C.D> <W.X.Y.Z >
```

The following table describes the parameters for this command.

no ip address parameters

Parameter	Description
<A.B.C.D>	The IP address to disable routing on.
<W.X.Y.Z >	The subnet mask to disable routing on.

The **no ip address** command is executed in the Interface Configuration command mode.

Multinetting

To add a secondary IP interface to a VLAN, known as Multinetting, use the following procedure:

Adding secondary IP interfaces

Step	Action
1	Put the switch into interface mode for the specific VLAN. `interface vlan <vlan #>`
2	Create a primary interface before adding secondary interfaces (if a primary interface has not yet been created). `ip address <ip address> <mask> [<mac offset>]`
3	Define a secondary IP interface on the VLAN.

```
ip address <ip address> <mask> [<mac offset>] secondary
```

—End—

Example Adding secondary IP interfaces to a VLAN

Primary and secondary interfaces must reside on different subnets. In the following example, 4.1.0.10 is the primary IP and 4.1.1.10 is the secondary IP.

```
interface vlan 4

ip address 4.1.0.10 255.255.255.0 6

ip address 4.1.0.10 255.255.255.0 6
```

Removing primary IP interfaces from a VLAN when secondary interfaces are configured

Step	Action
1	Put the switch into interface mode for the VLAN. `interface vlan <vlan #>`
2	Remove the secondary IP interface from the VLAN. `no ip address <ip address secondary> <mask>`
3	Remove the primary IP interface from the VLAN. `no ip address <ip address primary> <mask> [<mac offset>]`

—End—

Example removing primary IP interface from a VLAN when secondary interfaces are configured

In the following example, 4.1.0.10 is the primary IP and 4.1.1.10 is the secondary IP.

```
interface vlan 4

no ip address 4.1.0.10 255.255.255.0

no ip address 4.1.1.10 255.255.255.0
```

Example removing secondary IP interface only from a VLAN

```
interface vlan 4

no ip address 4.1.0.10 255.255.255.0
```

show vlan ip command

The **`show vlan ip`** command shows routable VLAN configurations.

The syntax for the **show vlan ip** command is:

```
show vlan ip [vid <1 - 4094>]
```

Substitute **<1 - 4094>** above with the VLAN ID of the VLAN to be displayed.

Static route commands

This section discusses the commands used to display and configure static routes on the Nortel Ethernet Routing Switch 5500 Series.

show ip route static command

The **show ip route static** command displays all static routes, whether these routes are active or inactive.

The syntax for the **show ip route static** command is:

```
show ip route static [<A.B.C.D>] [-s <O.P.Q.R> <W.X.Y.Z>]
```

The following table outlines the parameters for this command.

ip route static parameters

Parameters	Description
< A.B.C.D>	Enter IP address to display the static route for the specific IP address.
-s <O.P.Q.R>	Enter IP address for the subnet to display.
< W.X.Y.Z>	Enter subnet mask address for the subnet to display.

The **show ip route static** command is executed in the User EXEC command mode.

show ip route command

The **show ip route** command displays all active routes in the routing table.

Route entries appear in ascending order of the destination IP addresses.

The syntax for the **show ip route** command is:

```
show ip route [<A.B.C.D.|W.X.Y.Z.> <summary>]
```

show ip route command output

Ip Route								
DST	MASK	NEXT	COST	VLAN	PORT	PROT	TYPE	PRF
0.0.0.0	0.0.0.0	10.3.2.137	1	1	1/21	S	IB	5
2.2.2.0	255.255.255.0	2.2.2.2	1	2	----	C	DB	0

```
10.3.2.0    255.255.255.0   10.3.2.199   1        1        ----      C       DB       0

Total Routes: 3

TYPE Legend: I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp
Route, U=Unresolved Route, N=Not in HW
```

The following table outlines the parameters for this command.

show ip route parameters

Parameter	Description
<A.B.C.D>	Enter IP address to display the route for the specific IP address.
<W.X.Y.Z>	Enter subnet mask address for the subnet to display.
summary	Display a summary of IP route information.

The **show ip route** command is executed in the User EXEC command mode.

show ip route summary command

The **show ip route** summary command displays the software IP routing table.

The syntax for the **show ip route summary** command is:

```
show ip route summary
```

show ip route summary command output

```
------------------------
Connected routes :     65
Static routes    :     2
RIP routes       :     512
OSPF routes      :     512
------------------------
Total routes     :     1091
------------------------
```

The **show ip route summary** command is executed in the User EXEC command mode.

ip route command

The **ip route** command creates and configures a static route.

The syntax for the ip route command is:

```
ip route <A.B.C.D> <W.X.Y.Z> <O.P.Q.R> <1-65535>
```

The following table outlines the parameters for this command.

ip route parameters

Parameter	Description
<A.B.C.D>	Enter IP address of the destination point of the route being added.
<W.X.Y.Z>	Enter subnet mask address of the destination node for the route being added.
<O.P.Q.R>	Enter the IP address of the next hop of the route being added.
<1 - 65535>	Enter the weight, or cost, of the route being added.

The **ip route** command is executed in the Global Configuration command mode.

no ip route command

The **no ip route** command removes a static route.

The syntax for the **no ip route** command is:

```
no ip route <A.B.C.D> <W.X.Y.Z> <O.P.Q.R>
```

The following table outlines the parameters for this command.

no ip route parameters

Parameters	Description
<A.B.C.D>	Enter IP address of the destination point of the route being removed.
<W.X.Y.Z>	Enter subnet mask address of the destination node for the route being removed.
<O.P.Q.R>	Enter the IP address of the next hop of the route being removed.

The **no ip route** command is executed in the Global Configuration command mode.

ip route enable command

The **ip route enable** command enables a static route.

The syntax for the **ip route enable** command is:

```
ip route <A.B.C.D> <W.X.Y.Z> <O.P.Q.R> enable
```

The following table describes the parameters for this command.

ip route enable parameters

Parameter	Description
<A.B.C.D>	Enter IP address of the destination point of the route being enabled.
<W.X.Y.Z>	Enter subnet mask address of the destination node for the route being enabled.
<O.P.Q.R>	Enter the IP address of the next hop of the route being enabled.

The **`ip route enable`** command is executed in the Global Configuration command mode.

ip route disable command

The **`ip route disable`** command disables a static route.

The syntax for the **`ip route disable`** command is:

```
ip route <A.B.C.D> <W.X.Y.Z> <O.P.Q.R> disable
```

The following table describes the parameters for this command.

ip route disable parameters

Parameter	Description
<A.B.C.D>	Enter IP address of the destination point of the route being disabled.
<W.X.Y.Z>	Enter subnet mask address of the destination node for the route being disabled.
<O.P.Q.R>	Enter the IP address of the next hop of the route being disabled.

The **`ip route disable`** command is executed in the Global Configuration command mode.

traceroute command

The **`traceroute`** command displays the route taken by IP packets to a specified host.

> ***Note:*** The **`traceroute`** command, when applied to a stack, can be executed only on the base unit.

TIP: Type **CTRL+C** to interrupt the command.

The syntax for the **`traceroute`** command is:

```
traceroute <Hostname|A.B.C.D.|ip> <-m> <-p> <-q> <-v> <-w>
<1-1464>
```

The following table describes the parameters for this command.

traceroute parameters

Parameter	Description
Hostname	Enter the name of the remote host.
A.B.C.D.	Enter the A.B.C.D. name of the remote host.
ip	Enter the IP address of the remote host.
-m	Specifies the maximum time to live (ttl). The value for this parameter is in the rage from 1-255. The default value is 10. Example: **`traceroute 10.3.2.134 -m 10`**
-p	Specifies the base UDP port number. The value for this parameter is in the range from 0-65535. Example: **`traceroute 1.2.3.4 -p 87`**
-q	Specifies the number of probes per time to live. The value for this parameter is in the range from 1-255. The default value is 3. Example: **`traceroute 10.3.2.134 -q 3`**
-v	Specifies verbose mode. Example: **`traceroute 10.3.2.134 -v`**
-w	Specifies the wait time per probe. The value for this parameter is in the range from 1-255. The default value is 5 seconds. Example: **`traceroute 10.3.2.134 -w 15`**
<1-1464>	Specifies the UDP probe packet size. **TIP**: probe packet size is 40 plus specified data length in bytes. Example: **`traceroute 10.3.2.134 -w 60`**

ip route weight command

The **`ip route weight`** command changes the weight, or cost, of a static route.

The syntax for the **`ip route weight`** command is:

```
ip route <A.B.C.D> <W.X.Y.Z> <O.P.Q.R> weight <1-65535>
```

The following table outlines the parameters for this command.

ip route weight parameters

Parameter	Description
<A.B.C.D>	Enter IP address of the destination point of the route being modified.
<W.X.Y.Z>	Enter subnet mask address of the destination node for the route being modified.

Parameter	Description
<O.P.Q.R>	Enter the IP address of the next hop of the route being modified.
<1 - 65535>	Enter the new weight, or cost, of the static route.

The **ip route weight** command is executed in the Global Configuration command mode.

Address Resolution Protocol (ARP) commands

Use the CLI to display, create, configure, and remove ARP entries.

show arp command

The **show arp-table** command displays ARP entries.

The syntax for the **show arp-table** command is:

```
show arp-table [<A.B.C.D>]
```

Substitute **<A.B.C.D>** above with the IP address of the ARP table to be displayed.

The **show arp-table** command is executed in the Global Configuration command mode.

show ip arp command

The **show ip arp** command displays the IP addresses of ARP entries.

The syntax for the **show ip arp** command is:

```
show ip arp [<-s> <A.B.C.D.|W.X.Y.Z.>] [<static>]
```

The following table outlines the parameters for this command.

show ip arp parameters

Parameter	Description
-s	Specify the subnet of the ARP entries to be displayed.
<A.B.C.D>	Specify the IP address of the ARP entry to be displayed. This option is invalid if the switch is not in Layer 3 mode.
<W.X.Y.Z>	Enter subnet mask address in dotted decimal notation.
static	Display the software ARP table - all configured static entries, including those without a valid route.

The **show ip arp** command is executed in the Global Configuration command mode.

show ip arp static command

The **show ip arp static** command displays all configured static entries in an ARP table, including those without a valid route.

The syntax for the **show ip arp static** command is:

```
show ip arp static
```

The **show ip arp static** command can be executed in any command mode.

show ip arp static command output

IP ARP				
IP Address	Age (min)	MAC Address	VLAN-Unit/Port/Trunk	Flags
10.3.2.198	0	00:00:00:00:01:99	VLAN#1-1/1	S
Total ARP entries: 1				
Flags Legend: S=Static, D=Dynamic, L=Local, B=Broadcast				

ip arp command

The **ip arp** command creates and enables a static ARP entry. The requested information for connection to the device must be supplied.

The syntax for the **ip arp** command is:

```
ip arp <A.B.C.D> <aa:bb:cc:dd:ee:ff> <unit / port> [vid
<1-4094>]
```

The following table outlines the parameters for this command.

ip arp parameters

Parameters	Description
<A.B.C.D>	Enter the IP address of the device being set as a static ARP entry.
<aa:bb:cc:dd:ee:ff>	Enter the MAC address of the device being set as a static ARP entry.
<unit / port>	Enter the unit and port number of the device being set as a static ARP entry.
vid <1 - 4094>	Enter the VLAN ID to which the static ARP entry is being added to.

The **ip arp** command is executed in the Global Configuration command mode.

no ip arp command

The **no ip arp** command removes an ARP entry.

The syntax for the **no ip arp** command is:

```
no ip arp <A.B.C.D>
```

Substitute **<A.B.C.D>** above with the IP address of the static ARP entry to remove.

The **no ip arp** command is executed in the Global Configuration command mode.

ip arp timeout command

The **ip arp timeout** command configures an aging time for the ARP entries.

The syntax for the **ip arp timeout** command is:

```
ip arp timeout <5-360>
```

Substitute **<5-360>** above with the amount of time in minutes before an ARP entry ages out. The default value is 360 minutes.

The **ip arp timeout** command is executed in the Global Configuration command mode.

Proxy ARP commands

This section outlines the commands used to configure and manage Proxy ARP on the Nortel Ethernet Routing Switch 5500 Series.

ip arp-proxy command

The **ip arp-proxy** command is used to enable proxy ARP functionality on the switch

The syntax of the **ip arp-proxy** command is:

```
ip arp-proxy enable
```

The **ip arp-proxy** command is executed in the Layer 3 IP VLAN Interface Configuration mode.

no ip arp-proxy command

The **no ip arp-proxy** command is used to disable proxy ARP functionality on the switch.

The syntax of the **no ip arp-proxy** command is:

```
no ip arp-proxy [enable]
```

The **no ip arp-proxy** command is executed in the Layer 3 IP VLAN Interface Configuration mode.

default ip arp-proxy command

The **default ip arp-proxy** command is used to return the switch to the default proxy ARP settings.

The syntax of the **default ip arp-proxy** command is:

```
default ip arp-proxy [enable]
```

The **default ip arp-proxy** command is executed in the Layer 3 IP VLAN Interface Configuration mode.

show ip arp-proxy interface command

The **show ip arp-proxy interface** command is used to display the status of proxy ARP on an interface.

The syntax of the **show ip arp-proxy interface** command is:

```
show ip arp-proxy interface [vlan <vlan_id>]
```

The **show ip arp-proxy interface** command is executed in the User EXEC mode.

Routing Information Protocol (RIP) commands

This section describes the CLI commands used to configure and manage the Routing Information Protocol (RIP) on the Nortel Ethernet Routing Switch 5500 Series. RIP is a distance vector protocol used to dynamically discover network routes based on information passed between routers in the network. RIP is useful in network environments where using static route administration would be difficult.

router rip enable command

The **router rip enable** command is used to globally enable RIP on the switch. RIP must be globally enabled on the switch before it becomes operational.

The syntax of the **router rip enable** command is:

```
router rip enable
```

The **router rip enable** command is executed in the Global Configuration command mode.

router rip command

The **router rip** command is used to enter the Router Configuration mode for RIP. Router Configuration mode is used to configure various aspects of RIP, OSPF (**router ospf** command), and VRRP (**router vrrp** command).

The syntax of the **router rip** command is:

```
router rip
```

The **router rip** command is executed in the Global Configuration command mode.

network command

The **network** command is used to enable RIP on an IP interface.

The syntax of the **network** command is:

```
network <ip_address>
```

The **<ip_address>** parameter represents the IP address of the interface to be configured.

The **network** command is executed in the Router Configuration mode.

no network command

The **no network** command is used to disable RIP on an IP interface.

The syntax of the **no network** command is:

```
no network <ip_address>
```

The **<ip_address>** parameter represents the IP address of the interface to be disabled.

The **no network** command is executed in the Router Configuration mode.

timers basic holddown command

The **timers basic holddown** command is used to set the RIP holddown timer.

The syntax of the **timers basic holddown** command is:

```
timers basic holddown <timer_value>
```

The **<timer_value>** parameter represents a value between 0 and 360 seconds.

The **timers basic holddown** command is executed in the Router Configuration mode.

timers basic timeout command

The **timers basic timeout** command is used to set the RIP timeout timer.

The syntax of the **timers basic timeout** command is:

```
timers basic timeout <timer_value>
```

The **<timer_value>** parameter represents a value between 15 and 259200 seconds.

The **timers basic timeout** command is executed in the Router Configuration mode.

timers basic update command

The **timers basic update** command is used to set the RIP update timer.

The syntax of the **timers basic update** command is:

```
timers basic update <timer_value>
```

The **<timer_value>** parameter represents a value between 0 and 360 seconds.

The **default timers basic update** command is executed in the Router Configuration mode.

ip rip advertise-when-down command

The **ip rip advertise-when-down** command is used to enable RIP advertisements on the interface being configured even when that interface is not operational. The subnet on which the switch has a RIP enabled interface is advertised even if that particular network is no longer connected (no link in the connected VLAN is in the Link-Up state). This setting will take effect whenever the value is changed by the user or after the first Link-Down transition.

The syntax of the **ip rip advertise-when-down** command is:

```
ip rip advertise-when-down {enable}
```

Advertise when down functionality is disabled by default.

The **ip rip advertise-when-down** command is executed in the Interface Configuration mode.

no ip rip advertise-when-down command

The **ip rip advertise-when-down** command is used to disable RIP advertisements on the interface being configured even when that interface is not operational.

The syntax of the **no ip rip advertise-when-down** command is:

```
no ip rip advertise-when-down {enable}
```

The **no ip rip advertise-when-down** command is executed in the Interface Configuration mode.

ip rip auto-aggregation command

The **ip rip auto-aggregation** command is used to enable auto aggregation on the RIP interface. This allows for the automatic aggregation of routes to their natural net mask when they are advertised on an interface in a different class network.

The syntax of the **ip rip auto-aggregation** command is:

```
ip rip auto-aggregation {enable}
```

Auto aggregation is disabled by default.

The **ip rip auto-aggregation** command is executed in the Interface Configuration mode.

no ip rip auto-aggregation command

The **no ip rip auto-aggregation** command is used to disable auto-aggregation on the RIP interface.

The syntax of the **no ip rip auto-aggregation** command is:

```
no ip rip auto-aggregation {enable}
```

The **no ip rip auto-aggregation** command is executed in the Interface Configuration mode.

ip rip cost command

The **ip rip cost** command is used to set the administrative path cost of the interface.

The syntax of the **ip rip cost** command is:

```
ip rip cost <path_cost>
```

The **<path_cost>** parameter represents a value between 1 and 15.

The default path cost is 1.

The **ip rip cost** command is executed in the Interface Configuration mode.

ip rip default-listen command

The **ip rip default-listen** command is used to enable the acceptance of default route advertisements.

The syntax of the **ip rip default-listen** command is:

```
ip rip default-listen {enable}
```

The **ip rip default-listen** command is executed in the Interface Configuration mode.

no ip rip default-listen command

The **no ip rip default-listen** command is used to disable the acceptance of default route advertisements.

The syntax of the **no ip rip default-listen** command is:

```
no ip rip default-listen {enable}
```

The **no ip rip default-listen** command is executed in the Interface Configuration mode.

ip rip default-supply command

The **ip rip default-supply** command is used to enable the advertisement of default routes on the interface.

The syntax of the **ip rip default-supply** command is:

```
ip rip default-supply {enable}
```

The **ip rip default-supply** command is executed in the Interface Configuration mode.

no ip rip default-supply command

The **no ip rip default-supply** command is used to disable the advertisement of default routes on the interface.

The syntax of the **no ip rip default-supply** command is:

```
no ip rip default-supply {enable}
```

The **no ip rip default-supply** command is executed in the Interface Configuration mode.

ip rip holddown command

The **ip rip holddown** command is used to set the value of the holddown timer on the RIP interface.

The syntax of the **ip rip holddown** command is:

```
ip rip holddown <timer_value>
```

The **<timer_value>** parameter is an integer value between 0 and 360 seconds.

The **ip rip holddown** command is executed in the Interface Configuration mode.

ip rip in-policy command

The **ip rip in-policy** command is used to add an in policy to this RIP interface.

The syntax of the **ip rip in-policy** command is:

```
ip rip in-policy <policy_name>
```

The **<policy_name>** parameter represents the name of a previously configured switch policy.

The **ip rip in-policy** command is executed in the Interface Configuration mode.

no ip rip in-policy command

The **no ip rip in-policy** command is used to remove a in policy for the RIP interface.

The syntax of the **no ip rip in-policy** command is:

```
no ip rip in-policy <policy_name>
```

The **<policy_name>** parameter represents the name of a previously configured switch policy.

The **no ip rip in-policy** command is executed in the Interface Configuration mode.

ip rip listen command

The **ip rip listen** command is used to allow this interface to listen for RIP advertisements.

The syntax of the **ip rip listen** command is:

```
ip rip listen {enable}
```

The **ip rip listen** command is executed in the Interface Configuration mode.

no ip rip listen command

The **no ip rip listen** command is used to prevent this interface from listening for RIP advertisements.

The syntax of the **no ip rip listen** command is:

```
ip rip listen {enable}
```

The **no ip rip listen** command is executed in the Interface Configuration mode.

ip rip out-policy command

The **ip rip out-policy** command is used to add an out policy to this RIP interface.

The syntax of the **ip rip out-policy** command is:

```
ip rip out-policy <policy_name>
```

The **<policy_name>** parameter represents the name of a previously configured switch policy.

The **ip rip out-policy** command is executed in the Interface Configuration mode.

no ip rip out-policy command

The **no ip rip out-policy** command is used to remove an out policy from the RIP interface.

The syntax of the **no ip rip out-policy** command is:

```
no ip rip out-policy <policy_name>
```

The **<policy_name>** parameter represents the name of a previously configured switch policy.

The **no ip rip out-policy** command is executed in the Interface Configuration mode.

ip rip poison command

The **ip rip poison** command is used to enable poison reverse on this RIP interface.

The syntax of the **ip rip poison** command is:

```
ip rip poison {enable}
```

The **ip rip poison** command is executed in the Interface Configuration mode.

no ip rip poison command

The **no ip rip poison** command is used to disable poison reverse on this RIP interface.

The syntax of the **no ip rip poison** command is:

```
no ip rip poison {enable}
```

The **no ip rip poison** command is executed in the Interface Configuration mode.

ip rip proxy-announce command

The **ip rip proxy-announce** command is used to enable proxy announcements on this RIP interface. When proxy announcements are enabled, the source of a route and its next hop are treated as the same when processing received updates. So, instead of the advertising router being used as the source, the next hop is.

The syntax of the **ip rip proxy-announce** command is:

```
ip rip proxy-announce {enable}
```

Proxy announcements are disabled by default.

The **ip rip proxy-announce** command is executed in the Interface Configuration mode.

no ip rip proxy-announce command

The **no ip rip proxy-announce** command is used to disable proxy announcements on this RIP interface.

The syntax of the **no ip rip proxy-announce** command is:

```
no ip rip proxy-announce {enable}
```

The **no ip rip proxy-announce** command is executed in the Interface Configuration mode.

ip rip receive command

The **ip rip receive** command is used to set the RIP version received on this interface.

The syntax of the **ip rip receive** command is:

```
ip rip receive version <rip_version>
```

The **<rip_version>** parameter indicates the RIP version. The valid values for this parameter are:

- rip1
- rip1orrip2
- rip2

The **ip rip receive** command is executed in the Interface Configuration mode.

ip rip send command

The **ip rip send** command is used to set the RIP version sent on this interface.

The syntax of the **ip rip send** command is:

```
ip rip send version <rip_version>
```

The **<rip_version>** parameter indicates the RIP version. The valid values for this parameter are:

- notsend
- rip1
- rip1comp
- rip2

The **ip rip send** command is executed in the Interface Configuration mode.

ip rip supply command

The **ip rip supply** command is used to enable RIP route advertisement on this interface.

The syntax of the **ip rip supply** command is:

```
ip rip supply {enable}
```

The **ip rip supply** command is executed in the Interface Configuration mode.

no ip rip supply command

The **no ip rip supply** command is used to disable RIP route advertisement on this interface.

The syntax of the **no ip rip supply** command is:

```
no ip rip supply {enable}
```

The **no ip rip supply** command is executed in the Interface Configuration mode.

ip rip timeout command

The **ip rip timeout** command is used to set the RIP timeout value on this interface.

The syntax of the **ip rip timeout** command is:

```
ip rip timeout <timer_value>
```

The **<timer_value>** parameter is an integer value between 15 and 259200 seconds.

The default timeout value is 180 seconds.

The command is executed in the Interface Configuration mode.

ip rip triggered command

The **ip rip triggered** command is used to enable triggered updates on this RIP interface.

The syntax of the **ip rip triggered** command is:

```
ip rip triggered {enable}
```

The **ip rip triggered** command is executed in the Interface Configuration mode.

no ip rip triggered command

The **no ip rip triggered** command is used to disable triggered updates on this RIP interface.

The syntax of the **no ip rip triggered** command is:

```
no ip rip triggered {enable}
```

The **no ip rip triggered** command is executed in the Interface Configuration mode.

show ip rip command

The **show ip rip** command is used to display configuration and statistical information about RIP.

The syntax of the **show ip rip** command is:

```
show ip rip [interface]
```

Use the interface key word to display RIP statistics by interface. Omission of this key word displays general RIP information

The **show ip rip** command is executed in the Global Configuration mode.

default router rip command

The **default router rip** command is used to return the switch to the default global RIP state (disabled).

The syntax of the **default router rip** command is:

```
default router rip enable
```

The **default router rip** command is executed in the Router Configuration mode.

default default-metric command

The **default default-metric** command is used to return the switch to the factory default RIP default import metric.

The syntax of the **default default-metric** command is:

```
default default-metric
```

The **default default-metric** command is executed in the Router Configuration mode.

default timers basic holddown command

The **default timers basic holddown** command is used to return the switch to the factory default RIP holddown timer.

The syntax of the **default timers basic holddown** command is:

```
default timers basic holddown
```

The **default timers basic holddown** command is executed in the Router Configuration mode.

default timers basic timeout command

The **default timers basic timeout** command is used to return the switch to the factory default RIP timeout timer.

The syntax of the **default timers basic timeout** command is:

```
default timers basic timeout
```

The **default timers basic timeout** command is executed in the Router Configuration mode.

default timers basic update command

The **default timers basic update** command is used to return the switch to the factory default RIP update timer.

The syntax of the **default timers basic update** command is:

```
default timers basic update
```

The **default timers basic update** command is executed in the Router Configuration mode.

default-metric command

The **default-metric** command is used to set the default RIP metric value.

The syntax of the **default-metric** command is:

```
default-metric <metric_value>
```

The **<metric_value>** parameter is an integer value between 0 and 15.

The **default-metric** command is executed in the Router Configuration mode.

default ip rip advertise-when-down command

The **default ip rip advertise-when-down** command is used to restore the default RIP advertise when down setting for the interface (disabled).

The syntax of the **default ip rip advertise-when-down** command is:

```
default ip rip advertise-when-down enable
```

The **default ip rip advertise-when-down** command is executed in the Interface Configuration mode.

default ip rip auto-aggregation command

The **default ip rip auto-aggregation** command is used to restore the default RIP auto aggregation setting for the interface (disabled).

The syntax of the **default ip rip auto-aggregation** command is:

```
default ip rip auto-aggregation enable
```

The **default ip rip auto-aggregation** command is executed in the Interface Configuration mode.

default ip rip cost command

The **default ip rip cost** command is used to restore the default RIP costing settings for the interface.

The syntax of the **default ip rip cost** command is:

```
default ip rip cost [[out-policy <policy_name>] | [poison
enable] | [proxy-announce enable] | [receive <rip_version>]
| [send <rip_version>] | [supply enable] | [timeout] |
[triggered enable]]
```

The **default ip rip cost** command is executed in the Interface Configuration mode.

default ip rip default-listen command

The **default ip rip default-listen** command is used to restore the default RIP route listening setting for the interface (disabled).

The syntax of the **default ip rip default-listen** command is:

```
default ip rip default-listen enable
```

The **default ip rip default-listen** command is executed in the Interface Configuration mode.

default ip rip default-supply command

The **default ip rip default-supply** command is used to restore the default RIP route advertisement setting for the interface (disabled).

The syntax of the **default ip rip default-supply** command is:

```
default ip rip default-supply enable
```

The **default ip rip default-supply** command is executed in the Interface Configuration mode.

default ip rip enable command

The **default ip rip enable** command is used to globally disable RIP on the interface.

The syntax of the **default ip rip enable** command is:

```
default ip rip enable
```

The **default ip rip enable** command is executed in the Interface Configuration mode.

default ip rip holddown command

The **default ip rip holddown** command is used to restore the default RIP holddown setting for the interface.

The syntax of the **default ip rip holddown** command is:

```
default ip rip holddown
```

The **default ip rip holddown** command is executed in the Interface Configuration mode.

default ip rip in-policy command

The **default ip rip in-policy** command is used to delete the in policy associated with this interface.

The syntax of the **default ip rip in-policy** command is:

```
default ip rip in-policy <policy_name>
```

The **default ip rip in-policy** command is executed in the Interface Configuration mode.

default ip rip listen command

The **default ip rip listen** command is used to set the ip rip listen to the default value which is enabled.

The syntax of the **default ip rip listen** command is:

```
default ip rip listen enable
```

The **default ip rip listen** command is executed in the Interface Configuration mode.

default ip rip out-policy command

The **default ip rip out-policy** command is used to delete the out policy associated with this interface.

The syntax of the **default ip rip out-policy** command is:

```
default ip rip out-policy <policy_name>
```

The **default ip rip out-policy** command is executed in the Interface Configuration mode.

default ip rip poison command

The **default ip rip poison** command is used to disable RIP poison reverse on the interface.

The syntax of the **default ip rip poison** command is:

```
default ip rip poison enable
```

The **default ip rip poison** command is executed in the Interface Configuration mode.

default ip rip proxy-announce command

The **default ip rip proxy-announce** command is used to disable proxy announcement on the interface.

The syntax of the **default ip rip proxy-announce** command is:

```
default ip rip proxy-announce enable
```

The **default ip rip proxy-announce** command is executed in the Interface Configuration mode.

default ip rip receive command

The **default ip rip receive** command is used to set the default RIP version to listen to on this interface.

The syntax of the **default ip rip receive** command is:

```
default ip rip receive <rip_version>
```

The **default ip rip receive** command is executed in the Interface Configuration mode.

default ip rip send command

The **default ip rip send** command is used to set the default RIP version to send on this interface.

The syntax of the **default ip rip send** command is:

```
default ip rip send <rip_version>
```

The **default ip rip send** command is executed in the Interface Configuration mode.

default ip rip supply command

The **default ip rip supply** command is used to set ip rip supply to the default value which is enabled.

The syntax of the **default ip rip supply** command is:

```
default ip rip supply enable
```

The **default ip rip supply** command is executed in the Interface Configuration mode.

default ip rip timeout command

The **default ip rip timeout** command is used to restore the default RIP timeout setting for the interface.

The syntax of the **default ip rip timeout** command is:

```
default ip rip timeout
```

The **default ip rip timeout** command is executed in the Interface Configuration mode.

default ip rip triggered command

The **default ip rip triggered** command is used disabled triggered updates on this switch.

The syntax of the **default ip rip triggered** command is:

```
default ip rip triggered enable
```

The **default ip rip triggered** command is executed in the Interface Configuration mode.

Open Shortest Path First (OSPF) commands

This section describes the CLI commands used to configure and manage the Open Shortest Path First (OSPF) protocol on the Nortel Ethernet Routing Switch 5500 Series. The Open Shortest Path First (OSPF) Protocol is an Interior Gateway Protocol (IGP) that distributes routing information between routers belonging to a single *autonomous system* (AS). Intended for use in large networks, OSPF is a link-state protocol which supports IP subnetting and the tagging of externally-derived routing information.

> ***Note:*** OSPF commands used during the configuration and management of VLANs in the Interface Configuration mode can be used to configure *any* VLAN regardless of the one used to log into the command mode. Insert the keyword **vlan** with the number of the VLAN to be configured after the command keywords **ip ospf**. The current VLAN will remain at the one used to log into the Interface Configuration command mode after the command execution.

ip ospf apply accept command

The **ip ospf apply accept** command is used to apply OSPF accept policies to the switch.

The syntax of the **ip ospf apply accept** command is:

```
ip ospf apply accept
```

The **ip ospf apply accept** command is executed in the Global Configuration mode.

ip ospf apply redistribute direct command

The **ip ospf apply redistribute direct** command is used to apply only direct OSPF redistribution configuration to the switch.

The syntax of the **ip ospf apply redistribute direct** command is:

```
ip ospf apply redistribute direct
```

The **ip ospf apply redistribute direct** command is executed in the Global Configuration mode.

ip ospf apply redistribute rip command

The **ip ospf apply redistribute rip** command is used to apply only RIP OSPF redistribution configuration on the switch.

The syntax of the **ip ospf apply redistribute rip** command is:

```
ip ospf apply redistribute rip
```

The **ip ospf apply redistribute rip** command is executed in the Global Configuration mode.

ip ospf apply redistribute static command

The **ip ospf apply redistribute static** command is used to apply only static OSPF redistribution configuration on the switch.

The syntax of the **ip ospf apply redistribute static** command is:

```
ip ospf apply redistribute static
```

The **ip ospf apply redistribute static** command is executed in the Global Configuration mode.

ip ospf spf-run command

The **ip ospf spf-run** command is used to immediately initiate an SPF run upon holddown timer expiration to update the link state database.

The syntax of the **ip ospf spf-run** command is:

```
ip ospf spf-run
```

The **ip ospf spf-run** command is executed in the Global Configuration mode.

router ospf enable command

The **router ospf enable** command is used to enable OSPF globally on the switch.

The syntax of the **router ospf enable** command is:

```
router ospf enable
```

The **router ospf enable** command is executed in the Global Configuration mode.

no router ospf enable command

The **no router ospf enable** command is used to disable OSPF globally on the switch.

The syntax of the **no router ospf enable** command is:

```
no router ospf enable
```

The **no router ospf enable** command is executed in the Global Configuration mode.

router ospf command

The **router ospf** command is used to place the switch into Router Configuration mode for the purposes of OSPF configuration.

The syntax of the **router ospf** command is:

```
router ospf
```

The **router ospf** command is executed in the Global Configuration mode.

default router ospf command

The **default router ospf** command is used to return the switch to the default OSPF setting; which is disabled.

The syntax of the **default router ospf** command is:

```
default router ospf enable
```

The **default router ospf** command is executed in the Global Configuration mode.

accept adv-rtr command

The **accept adv-rtr** command is used to configure the router to accept advertisements from another router in the system.

The syntax of the **accept adv-rtr** command is:

```
accept adv-rtr <router_ip_address> [enable] [metric-type {any
| type1 | type2}] [route-policy {policy_name}]
```

The following table outlines the parameters for this command.

accept adv-rtr parameters

Parameter	Description
router_ip_address	This parameter represents the IP address of the router advertisements will be accepted from. The value *0.0.0.0* denotes that advertisements from all routers will be accepted.
enable	Enables the accept entry for the router specified in the **<ip_address>** parameter.
metric-type {any | type1 | type2}	Indicates the type of OSPF external routes that will be accepted from this router.
route-policy {policy_name}	Specifies the name of the route policy to be used for filtering external routes advertised by the specified advertising router before accepting them into the routing table.

The **accept adv-rtr** command is executed in the Router Configuration mode.

no accept adv-rtr command

The **no accept adv-rtr** command is used to configure the router to not accept advertisements from another router in the system.

The syntax of the **no accept adv-rtr** command is:

```
no accept adv-rtr <router_ip_address> enable
```

The **<router_ip_address>** parameter represents the address of the router from which advertisements will no longer be accepted. The value *0.0.0.0* denotes that advertisements from all routers will be blocked.

The **no accept adv-rtr** command is executed in the Router Configuration mode.

area command

The **area** command is used to configure OSPF area parameters.

The syntax of the **area** command is:

```
area <ip_address> [default-cost {0-16777215}] [import
{external | noexternal | nssa}] [import-summaries {enable}]
[range {subnet_mask} [{nssa-entlink | summary-link}]
```

```
[advertise-mode {no-summarize | summarize | suppress}]
[advertise-metric {0-65535}]]
```

The following table outlines the parameters for this command.

area parameters

Parameter	Description
ip_address	Specifies the Area ID expressed as IP address (A.B.C.D).
default-cost {0-16777215}	The default cost associated with an OSPF stub area.
import {external | noexternal | nssa}	The area's support for importing Autonomous System external link state advertisements.
import-summaries {enable}	Controls the import of summary link state advertisements into stub areas. This setting has no effect on other areas.
range {subnet_mask} [{nssa-entlink | summary-link}] [advertise-mode { no-summarize | summarize | suppress}] [advertise-metric {0-65535}]	Used to specify range parameters for the OSPF area.

The **area** command is executed in the Router Configuration mode.

> ***Note:*** The configuration of a totally stubby area (no summary advertising) is a two step process. First, define an area with the import flag set to *noexternal*. Second, disable import summaries in the same area with the command **no area <ip_address> import-summaries enable**.

no area command

The **no area** command is used to disable configured OSPF area parameters.

The syntax of the **no area** command is:

```
no area <ip_address> [import-summaries {enable} | range
{subnet_mask} {nssa-entlink | summary-link}]
```

The following table outlines the parameters for this command.

no area parameters

Parameter	Description
ip_address	Specifies the Area ID expressed as IP address (A.B.C.D).
import-summaries {enable}	Controls the import of summary link state advertisements into stub areas. This setting has no effect on other areas.
range {subnet_mask} {nssa-entlink | summary-link}	Used to specify range parameters for the OSPF area.

The **no area** command is executed in the Router Configuration mode.

> ***Note:*** The configuration of a totally stubby area (no summary advertising) is a two step process. First, define an area with the import flag set to *noexternal*. Second, disable import summaries in the same area with the command **no area <ip_address> import-summaries enable**.

as-boundary-router command

The **as-boundary-router** command is used to denote a router as an Autonomous System Boundary Router.

The syntax of the **as-boundary-router** command is:

```
as-boundary-router {enable}
```

The **as-boundary-router** command is executed in the Router Configuration mode.

no as-boundary-router command

The **no as-boundary-router** command is used to withdraw a router as an Autonomous System Boundary Router.

The syntax of the **no as-boundary-router** command is:

```
no as-boundary-router {enable}
```

The **no as-boundary-router** command is executed in the Router Configuration mode.

default-cost ethernet command

The **default-cost ethernet** command is used to define the default cost metric of an ethernet (10 Mbps) port.

The syntax of the **default-cost ethernet** command is:

```
default-cost ethernet <metric_value>
```

The **<metric_value>** parameter represents the cost value to assign to the port. This value is an integer between 1 and 65535.

The **default-cost ethernet** command is executed in the Router Configuration mode.

default-cost fast-ethernet command

The **default-cost fast-ethernet** command is used to define the default cost metric of a fast ethernet (100 Mbps) port.

The syntax of the **default-cost fast-ethernet** command is:

```
default-cost fast-ethernet <metric_value>
```

The **<metric_value>** parameter represents the cost value to assign to the port. This value is an integer between 1 and 65535.

The **default-cost fast-ethernet** command is executed in the Router Configuration mode.

default-cost gig-ethernet command

The **default-cost gig-ethernet** command is used to define the default cost metric of a gig ethernet (1000 Mbps) port.

The syntax of the **default-cost gig-ethernet** command is:

```
default-cost gig-ethernet <metric_value>
```

The **<metric_value>** parameter represents the cost value to assign to the port. This value is an integer between 1 and 65535.

The **default-cost gig-ethernet** command is executed in the Router Configuration mode.

default-cost ten-gig-ethernet command

The **default-cost ten-gig-ethernet** command is used to define the default cost metric of a ten gig ethernet (10000 Mbps) port.

The syntax of the **default-cost ten-gig-ethernet** command is:

```
default-cost ten-gig-ethernet <metric_value>
```

The **<metric_value>** parameter represents the cost value to assign to the port. This value is an integer between 1 and 65535.

The **default-cost ten-gig-ethernet** command is executed in the Router Configuration mode.

host-route command

Use the **host-route** command to add a host to a router. For more information about host routes, see "OSPF host route" (page 29).

The syntax for the **host-route** command is:

```
host-route <A.B.C.D.> metric <0-65535>
```

where <A.B.C.D.> is the host IP address and metric is an integer between 0 and 65535 representing the configured cost of the host

The **host-route** command is executed in the Router Configuration mode.

no host-route command

Use the **no host-route** command to delete a host from a router.

The syntax for the **no host-route** command is:

```
no host-route <A.B.C.D.>
```

where <A.B.C.D.> is the host IP address

The **no host-route** command is executed in the Router Configuration mode.

network command

The **network** command is used to enable OSPF routing on an interface and assign an OSPF interface to an area.

The syntax of the **network** command is:

```
network <ip_address> [area <ip_address>]
```

The following table describes the parameters of this command.

network parameters

Field	Description
<ip_address>	The IP address of interface to be enabled for OSPF routing.
area <area_Id>	The area assigned to the interface.

The **network** command is executed in the Router Configuration mode.

no network command

The **no network** command is used to disable OSPF routing on an interface.

The syntax of the **no network** command is:

```
no network <ip_address>
```

The **<ip_address>** parameter represents the IP address of the interface to be disabled.

The **no network** command is executed in the Router Configuration mode.

redistribute command

The **redistribute** command is used to configure OSPF route redistribution. Direct, RIP, and static route redistribution is currently supported.

The syntax of the **redistribute** command is:

```
redistribute <route_type> [enable] [metric <metric_value>]
[metric-type <metric_type>] [route-policy <policy_name>]
[subnets <subnet_setting>]
```

The parameters for this command are listed below.

redistribute parameters

Parameters	Description
<route_type>	The type of route to be configured. Valid options are **direct**, **rip**, and **static**.
<metric_value>	The metric value to associate with the route redistribution. This is an integer value between 0 and 65535.
<metric_type>	The metric type to associate with the route redistribution. Valid options are **type1** and **type2**.
<policy_name>	The route policy to associate with route redistribution. This is the name of an existing route policy.
<subnet_setting>	The subnet advertisement setting of this route redistribution. This determines whether individual subnets are advertised. Valid options are **allow** and **suppress**.

The **redistribute** command is executed in the Router Configuration mode.

no redistribute command

The **no redistribute** command is used to disable an OSPF route policy or OSPF route redistribution completely.

The syntax of the **no redistribute** command is:

```
redistribute <route_type> [enable] [route-policy
<policy_name>]
```

The parameters for this command are listed below.

no redistribute parameters

Parameters	Description
<route_type>	The type of route to be configured. Valid options are **direct**, **rip**, and **static**.
<policy_name>	The route policy to remove from the route redistribution. This is the name of an existing route policy.

The **no redistribute** command is executed in the Router Configuration mode.

rfc1583-compatibility command

The **rfc1583-compatibility** command is used to enable compatibility for RFC 1583 in the switch OSPF implementation.

The syntax of the **rfc1583-compatibility** command is:

```
rfc1583-compatibility enable
```

The **rfc1583-compatibility** command is executed in the Router Configuration mode.

no rfc1583-compatibility command

The **no rfc1583-compatibility** command is used to disable compatibility for RFC 1583 in the switch OSPF implementation.

The syntax of the **no rfc1583-compatibility** command is:

```
no rfc1583-compatibility enable
```

The **no rfc1583-compatibility** command is executed in the Router Configuration mode.

router-id command

The **router-id** command is used to set the identifier to the user-configured router ID, which is expressed in the form of an IP address.

The syntax of the **router-id** command is:

```
router-id <router_id>
```

The **<router_id>** parameter is used as the unique identifier for the router.

The **router-id** command is executed in the Router Configuration mode.

no router-id command

The **no router-id** command is used to reset the router ID to 0.0.0.0.

The syntax of the **no router-id** command is:

```
no router-id
```

The **no router-id** command is executed in the Router Configuration mode.

timers basic holddown command

The **timers basic holddown** command is used to configure the OSPF holddown timer.

The syntax of the **timers basic holddown** command is:

```
timers basic holddown <timer_value>
```

The **<timer_value>** parameter represents a second value between 3 and 60 seconds.

The command is executed in the Router Configuration mode.

trap command

The **trap** command is used to enable OSPF system traps.

The syntax of the **trap** command is:

```
trap enable
```

The **trap** command is executed in the Router Configuration mode.

no trap command

The **no trap** command is used to disable OSPF system traps.

The syntax of the **no trap** command is:

```
no trap enable
```

The **no trap** command is executed in the Router Configuration mode.

area virtual-link command

Use the **area virtual-link** command to create a virtual interface.

The syntax for the **area virtual-link** command is:

```
area virtual-link <A.B.C.D.> <W.X.Y.Z> {[authentication-key
<WORD>] [authentication-type {none|simple|message-digest}]
[primary-md5-key <1-255>] [dead-interval <0-2147483647>]
[hello-interval <1-65535>] [retransmit-interval <0-3600>]
[transit-delay <0-3600>]
```

area virtual-link parameters

Parameter	Description
<A.B.C.D.>	Specifies the transit area ID expressed as an IP address.
<A.B.C.D./0-32>	Specifies the neighbor router ID expressed as an IP address.
authentication-key <WORD>	Specifies the unique identifier assigned to the authentication key.
authentication-type	Specifies one of the following authentication types: • none • simple • password • message digest MD5 TIP: Up to 2 MD5 keys are allowed for message digest. The default authentication type is none.
primary-md5-key	Specifies the user-selected key used to encrypt OSPF protocol packets for transmission.
dead-interval	Specifies the time interval, in seconds, that a Hello packet has not been transmitted from the virtual interface before its neighbors declare it down. Expressed as an integer from 0-2147483647, the default dead interval value is 60 seconds.
hello-interval	Specifies the time interval, in seconds, between transmission of Hello packets from the virtual interface. Expressed as an integer from 1-65535, the hello-interval default value is 10 seconds.
retransmit-interval	Specifies the time interval, in seconds, between link stage advertisement retransmissions for adjacencies belonging to the virtual interface. Expressed as an integer from 0-3600, the default value is 5 seconds.
transit-delay	Specifies the estimated number of seconds required to transmit a link state update packet over the virtual interface. Expressed as an integer from 0-3600, the default value is 1 second.

The **`area vitual-link`** command is executed in the Router Configuration mode.

no area virtual-link command

Use the **`no area virtual-link`** command to delete a virtual interface.

The syntax for the **`no area virtual link`** command is:

```
no area virtual-link <A.B.C.D.> <W.X.Y.Z> [authentication-
key]
```

no area virtual-link command parameters

Parameter	Description
<A.B.C.D.>	Specifies the transit area Id expressed as an IP address.
<W.X.Y.Z>	Specifies the neighbor router ID expressed as an IP address.
authentication-key	Specifies the unique identifier assigned to the authentication key

The **no area virtual-link** command is executed in the Router Configuration mode.

area virtual-link message-digest-key command

Use the **area virtual-link message-digest-key** command to create a virtual interface message digest key.

The syntax for the **area virtual-link message-digest-key** command is:

```
area virtual-link message-digest-key <A.B.C.D.> <A.B.C.D./0-
32> <1-255> md5-key <WORD>
```

area virtual-link message-digest key command parameters

Parameter	Description
<A.B.C.D.>	Specifies the transit area Id expressed as an IP address.
<W.X.Y.Z>	Specifies the neighbor router ID expressed as an IP address.
<1-255>	Specifies the primary MD5 key value, expressed as an integer from 1-255.
md5-key <WORD>	Specifies the user-selected key used to encrypt OSPF protocol packets for transmission.

The **area virtual-link message-digest-key** command is executed in the Router Configuration mode.

no area virtual-link message-digest-key command

Use the **no area virtual-link message-digest-key** command to delete a virtual interface message digest key.

The syntax for the **no area virtual-link message-digest-key** command is:

```
no area virtual-link message-digest-key <A.B.C.D.> <W.X.Y.Z>
<1-255>
```

no area virtual-link message-digest-key command parameters

Parameter	Description
<A.B.C.D.>	Specifies the transit area ID expressed as an IP address.
<W.X.Y.Z>	Specifies the neighbor router ID expressed as an IP address.
<1-255>	Specifies the primary MD5 key value, expressed as an integer from 1-255.

The **no area virtual-link message-digest-key** command is executed in the Router Configuration mode.

auto-vlink command

Use the auto-vlink command to enable global automatic Virtual Link creation. For more information about Virtual Link, see "OSPF virtual link" (page 31)

The syntax for the **auto-vlink** command is:

```
auto-vlink
```

The **auto-vlink** command is executed in the Router Configuration mode.

no auto-vlink command

Use the **no auto-vlink** command to disable global automatic Virtual Link creation.

The syntax for the **no auto-vlink** command is:

```
no auto-vlink
```

The **no auto-vlink** command is executed in the Router Configuration mode.

ip ospf advertise-when-down command

The **ip ospf advertise-when-down** command is used to enable advertisement of the OSPF interface even when the interface is operationally unavailable.

The syntax of the **ip ospf advertise-when-down** command is:

```
ip ospf advertise-when-down enable
```

The **ip ospf advertise-when-down** command is executed in the Interface Configuration mode.

ip ospf area command

The **ip ospf area** command is used to assign an interface to an OSPF area.

The syntax of the **ip ospf area** command is:

```
ip ospf area <ip_address>
```

The **<ip_address>** parameter represents the unique ID of the area to which the interface connects. An area ID of 0.0.0.0 indicates the OSPF area backbone and is created automatically by the switch.

The **ip ospf area** command is executed in the Interface Configuration mode.

ip ospf authentication-key command

The **ip ospf authentication-key** command is used to configure an interface authentication password.

The syntax of the **ip ospf authentication-key** command is:

```
ip opsf authentication-key <password>
```

The **<password>** parameter is the password to be configured. This password can be up to 8 characters in length.

The **ip opsf authentication-key** command is executed in the Interface Configuration mode.

ip ospf authentication-type command

The **ip ospf authentication-type** command is used to configure the interface authentication type.

The syntax of the **ip ospf authentication-type** command is:

```
ip ospf authentication-type {message-digest | simple | none}
```

The **ip ospf authentication-type** command is executed in the Interface Configuration mode.

ip ospf cost command

The **ip ospf cost** command is used to assign a cost to an interface.

The syntax of the **ip ospf cost** command is:

```
ip ospf cost <interface_cost>
```

The **<interface_cost>** parameter is the cost assigned to the interface. This is an integer value between 1 and 65535.

The **ip ospf cost** command is executed in the Interface Configuration mode.

ip ospf dead-interval command

The **ip ospf dead-interval** command is used to configure a dead interval for the interface. This is the interval of time that a Hello packet has not been transmitted from this interface before its neighbors declare it down.

The syntax of the **ip ospf dead-interval** command is:

```
ip ospf dead-interval <interval>
```

The **<interval>** parameter represents the amount of time in seconds to set this interval at. This is an integer value between 0 and 2147483647.

The **ip ospf dead-interval** command is executed in the Interface Configuration mode.

ip ospf hello-interval command

The **ip ospf hello-interval** command is used to configure the amount of time between transmission of hello packets from this interface.

The syntax of the **ip ospf hello-interval** command is:

```
ip ospf hello-interval <interval>
```

The **<interval>** parameter is the amount of time in seconds between hello packets. This is an integer value between 1 and 65535.

The **ip ospf hello-interval** command is executed in the Interface Configuration mode.

ip ospf mtu-ignore command

The **ip ospf mtu-ignore** command is used to instruct the interface to ignore the packet MTU size specified in *Database Descriptors*.

The syntax of the **ip ospf mtu-ignore** command is:

```
ip ospf mtu-ignore enable
```

The **ip ospf mtu-ignore** command is executed in the Interface Configuration mode.

ip ospf network command

The **ip ospf network** command is used to define the type of OSPF interface this interface is.

The syntax of the **ip ospf network** command is:

ip ospf network {broadcast | passive}

The **ip ospf network** command is executed in the Interface Configuration mode.

ip ospf primary-md5-key command

The **ip ospf primary-md5-key** command is used to configure the primary MD5 key to use for authentication in instances where interface authentication uses an MD5 key.

The syntax of the **ip ospf primary-md5-key** command is:

ip ospf primary-md5-key <key_value>

The **<key_value>** parameter is an integer value between 1 and 255.

The **ip ospf primary-md5-key** command is executed in the Interface Configuration mode.

ip ospf priority command

The **ip ospf priority** command is used to assign a priority to the interface for the purposes of Designated Router election.

The syntax of the **ip ospf priority** command is:

ip ospf priority <priority_value>

The **<priority_value>** parameter is the priority value assigned to the interface. This is an integer value between 0 and 255.

The **ip ospf priority** command is executed in the Interface Configuration mode.

ip ospf retransmit-interval command

The **ip ospf retransmit-interval** command is used to define the number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface.

The syntax of the **ip ospf retransmit-interval** command is:

ip ospf retransmit-interval <interval>

The **<interval>** parameter is the number of seconds between retransmissions. This is an integer value between 0 and 3600.

The **ip ospf retransmit-interval** command is executed in the Interface Configuration mode.

ip ospf transmit-delay command

The **ip ospf transmit-delay** command is used to define the transmit delay for this OSPF interface.

The syntax of the **ip ospf transmit-delay** command is:

```
ip ospf transmit-delay <interval>
```

The **<interval>** parameter is the transmit delay in seconds. This is an integer value between 0 and 3600.

The **ip ospf transmit-delay** command is executed in the Interface Configuration mode.

ip ospf message-digest-key command

The **ip ospf message-digest-key** command is used to define the MD5 keys referenced in the **ip ospf primary-md5-key** command.

The syntax of the **ip ospf message-digest-key** command is:

```
ip ospf message-digest-key <key_number> md5 <key_value>
```

The **<key_number>** parameter represents the MD5 key to be configured. This is an integer value between 1 and 255. The **<key_value>** parameter represents the value of the key being configured. This is a string value of up to 16 characters in length.

The **ip ospf message-digest-key** command is executed in the Interface Configuration mode.

OSPF show commands

OSPF functionality provides a wide range of commands used to display statistics and configured parameters for the router. These commands are available for use in any command mode. OSPF Show commands are outlined in the table below.

OSPF show commands

Command	Description
show ip ospf	Displays general information on OSPF configuration.
show ip ospf accept	Displays information on OSPF advertising routers.
show ip ospf area <ip_address>	Displays configuration information about the OSPF area specified in the **<ip_address>** parameter. Omitting this parameter displays information for all OSPF areas.

Command	Description
show ip ospf area-range <ip_address>	Displays configuration information about the OSPF area range specified in the **<ip_address>** parameter. Omitting this parameter displays information for all OSPF area ranges.
show ip ospf ase	Displays information about the OSPF Autonomous System external links state advertisements.
show ip ospf default	Displays OSPF default metrics associated with various port types.
show ip ospf default-cost	Displays the default costs associated with various port types.
show ip ospf ifstats <ip_address> {detail | mismatch}	Displays OSPF interface statistics. All parameters for this command are optional. Not specifying an address of an area will display statistics for the backbone area.
show ip ospf int-auth	Displays the authentication type and key for each OSPF interface.
show ip ospf int-timers	Displays the configured timers for each OSPF interface.
show ip ospf lsdb {adv-rtr <ip_address> | area <ip_address> | detail <ip_address> | lsa-type <type> | lsid <ip_address>}	Displays the link state database for the selected parameter.
show ip ospf neighbor	Displays information about the router's OSPF neighbors.
show ip ospf redistribute	Displays information about OSPF redistribution policies.
show ip ospf stats	Displays OSPF statistics. **TIP**: To clear OSPF statistics counters, execute the **`clear ip ospf counters`** command.
show ip ospf timer interface	Displays configured OSPF timers.
show ip ospf authentication interface	Displays interface MD5 authentication keys.
show ip ospf interface	Displays general OSPF interface information.
show ip ospf virtual-links	Displays OSPF virtual link information.
show ip ospf timer virtual-links	Displays OSPF transit delay, retransmit interval, hello interval and retransmit dead interval information for the virtual interface.
show ip ospf authentication virtual links	Displays virtual interface MD5 authentication keys.

Command	Description
show ip ospf virtual-neighbors	Displays general information about virtual neighbors.
show ip ospf host-route	Displays the host IP address and cost for a host route.

clear ip ospf counters command

The **clear ip ospf counters** command clears OSPF statistics counters, including mismatch counters.

TIP: If no VLAN is specified, the command clears OSPF global counters.

> ***Note:*** The **clear ip ospf counters** command is applicable only to the base unit in a stack.

The syntax for the **clear ip ospf counters** command is:

```
clear ip ospf counters <1-4094>
```

where the optional parameter <1-4094> is the VLAN ID.

The **clear ip ospf counters** command is executed in the Configuration mode.

Route policy commands

Route policies are a Nortel proprietary improvement on existing routing schemes. Using existing routing schemes, packets are forwarded based on routes that have been learned by the router through routing protocols such as RIP and OSPF or through the introduction of static routes. Route policies introduce the ability to forward packets based on rule sets created by the network administrator. These rule sets, or policies, are then applied to the learned or static routes.

This section describes the configuration and management of route policies using the Command Line Interface.

ip prefix-list command

The **ip prefix-list** command is used to configure up to four prefix lists for use in route policies.

The syntax of the **ip prefix-list** command is:

```
ip prefix-list <prefix_name> {<ip_address/mask> [ge
<mask_from>] [le <mask_to>] | name <new_prefix_name>}
```

The following table describes the parameters for this command.

ip prefix-list parameters

Parameter	Description
<prefix_name>	The name assigned to the prefix list.
<ip_address/mask>	The IP address and subnet mask of the prefix list. The subnet mask is expressed as a value between 0 and 32.
<mask_from>	The subnet range covered by the prefix list from the stated IP address.
<mask_to>	The subnet range covered by the prefix list to the stated IP address.
<new_prefix_name>	Used to assign a new name to previously configured prefix list.

The **ip prefix-list** command is executed in the Global Configuration mode.

route-map command

The **route-map** command is used to define route maps used in the configuration of route policies.

The syntax of the **route-map** command is:

```
route-map <map_name> [permit | deny] <sequence_number>
[enable] [match {interface <prefix_list> | next-hop
<prefix_list> | protocol <protocol_name> | route-
source <prefix_list> | route-type <route_type>}] [name
<new_map_name>] [set {injectlist <prefix_list> | mask
<ip_address> | metric <metric_value> | metric-type
<metric_type> | nssa-pbit enable}]
```

The following table outlines the parameters for this command.

route-map parameters

Field	Description
<map_name>	The name associated with this route map.
[permit | deny]	Specifies the action to be taken when this policy is selected for a specific route. A value of **permit** indicates that the route will be used while **deny** indicates that the route will be ignored.
<sequence_number>	The secondary index value assigned to individual policies inside a larger policy group.
enable	Indicates whether the policy is enabled. Disabled policies should not be used for routing.

<prefix_list>	Indicates a previously defined prefix list to be used with the command. This parameter is used with various options in this command.
<protocol_name>	The name of a protocol to be used. Options are direct, static, rip, ospf, and any. Multiple protocols can be specified by using a comma-separated list.
<route_type>	A route type to be used. Options are any, external, external-1, external-2, internal, and local.
<new_map_name>	A new name to be assigned to a previously configured route map.
<ip_address>	An IP address and subnet mask to be used.
<metric_value>	Indicates the value of the metric to be used while sending an update for routes. This is an integer value between 0 and 65535.
<metric_type>	Indicates the metric type for routes to be imported into the OSPF routing protocol. Options are type1 and type2.

The **route-map** command is executed in the Global Configuration mode.

ip rip in-policy command

The **ip rip in-policy** command is used to specify a RIP Accept (In) policy for an interface. This policy takes the form of a previously configured route map.

The syntax of the **ip rip in-policy** command is:

```
ip rip in-policy <rmap_name>
```

The **<rmap_name>** parameter represents the name of a previously configured route map.

The **ip rip in-policy** command is executed in the Interface Configuration mode.

ip rip out-policy command

The **ip rip out-policy** command is used to specify a RIP Announce (Out) policy for an interface. This policy takes the form of a previously configured route map.

The syntax of the **ip rip out-policy** command is:

```
ip rip out-policy <rmap_name>
```

The **<rmap_name>** parameter represents the name of a previously configured route map.

The **ip rip out-policy** command is executed in the Interface Configuration mode.

Virtual Router Redundancy Protocol (VRRP) commands

The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure that can occur when the single static default gateway router for an end station is lost.

This section describes the CLI commands used to configure VRRP.

router vrrp enable command

The **router vrrp enable** command is used to globally enable VRRP on a switch.

The syntax of the **router vrrp enable** command is:

```
router vrrp enable
```

The **router vrrp enable** command is executed in the Global Configuration mode.

no router vrrp enable command

The **no router vrrp enable** command is used to globally disable VRRP on a switch.

The syntax of the **no router vrrp enable** command is:

```
no router vrrp enable
```

The **no router vrrp enable** command is executed in the Global Configuration mode.

router vrrp command

The **router vrrp** command is used to place the switch into Router Configuration mode for the purposes of VRRP configuration.

The syntax of the **router vrrp** command is:

```
router vrrp
```

The **router vrrp** command is executed in the Global Configuration mode.

ping-virtual-address enable command

The **ping-virtual-address enable** command is used to enable ICMP echo replies from VRRP associated addresses.

The syntax of the **ping-virtual-address enable** command is:

```
ping-virtual-address enable
```

The **ping-virtual-address enable** command is executed in the Router Configuration mode.

no ping-virtual-address enable command

The **no ping-virtual-address enable** command is used to disable ICMP echo replies from VRRP associated addresses.

The syntax of the **no ping-virtual-address enable** command is:

```
no ping-virtual-address enable
```

The **no ping-virtual-address enable** command is executed in the Router Configuration mode.

send-trap enable command

The **send-trap enable** command is used to enable the sending of SNMP notifications after virtual router state changes.

The syntax of the **send-trap enable** command is:

```
send-trap enable
```

The **send-trap enable** command is executed in the Router Configuration mode.

no send-trap enable command

The **no send-trap enable** command is used to disable the sending of SNMP notifications after virtual router state changes.

The syntax of the **no send-trap enable** command is:

```
no send-trap enable
```

The **no send-trap enable** command is executed in the Router Configuration mode.

ip vrrp address command

The **ip vrrp address** command is used to associated an IP address with a virtual router ID.

The syntax of the **ip vrrp address** command is:

```
ip vrrp address <vr_id> <ip_address>
```

The **<vr_id>** parameter represents the virtual router being configured. This is a value between 1 and 255. The **<ip_address>** parameter represents the address to be used in the association.

The **ip vrrp address** command is executed in the Interface Configuration mode.

no ip vrrp address command

The **no ip vrrp address** command is used to delete the association of an IP address with a virtual router ID.

The syntax of the **no ip vrrp address** command is:

```
no ip vrrp address <vr_id> <ip_address>
```

The **<vr_id>** parameter represents the virtual router being configured. This is a value between 1 and 255. The **<ip_address>** parameter represents the address to be used in the association.

The **no ip vrrp address** command is executed in the Interface Configuration mode.

ip vrrp action command

The **ip vrrp action** command is used to define the action this interface will take when a holddown timer threshold has been reached.

The syntax of the **ip vrrp action** command is:

```
ip vrrp action <vr_id> {none | preempt}
```

The **<vr_id>** parameter represents the virtual router being configured. If **none** is selected as the action, no action is taken when a holddown timer threshold is reached. If **preempt** is selected as the action, the holddown timer is cancelled.

The **ip vrrp action** command is executed in the Interface Configuration mode.

ip vrrp adver-int command

The **ip vrrp adver-int** command is used to set the VRRP advertisement interval.

The syntax of the **ip vrrp adver-int** command is:

```
ip vrrp <vr_id> adver-int <interval>
```

The **<vr_id>** parameter represents the virtual router being configured. The **<interval>** parameter represents the advertisement interval in seconds. This is an integer value between 1 and 255.

The **ip vrrp adver-int** command is executed in the Interface Configuration mode.

ip vrrp backup-master command

The **ip vrrp backup-master** command is used to enable the VRRP backup / master functionality.

The syntax of the **ip vrrp backup-master** command is:

```
ip vrrp <vr_id> backup-master enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **ip vrrp backup-master** command is executed in the Interface Configuration mode.

no ip vrrp backup-master command

The **no ip vrrp backup-master** command is used to disable the VRRP backup / master functionality.

The syntax of the **no ip vrrp backup-master** command is:

```
no ip vrrp <vr_id> backup-master enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **no ip vrrp backup-master** command is executed in the Interface Configuration mode.

ip vrrp critical-ip command

The **ip vrrp critical-ip** command is used to enable the VRRP critical IP functionality.

The syntax of the **ip vrrp critical-ip** command is:

```
ip vrrp <vr_id> critical-ip enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **ip vrrp critical-ip** command is executed in the Interface Configuration mode.

no ip vrrp critical-ip command

The **no ip vrrp critical-ip** command is used to disable the VRRP critical IP functionality.

The syntax of the **no ip vrrp critical-ip** command is:

```
no ip vrrp <vr_id> critical-ip enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **no ip vrrp critical-ip** command is executed in the Interface Configuration mode.

ip vrrp critical-ip-addr command

The **ip vrrp critical-ip-addr** command is used to set the IP address used with the VRRP critical IP functionality.

The syntax of the **ip vrrp critical-ip-addr** command is:

```
ip vrrp <vr_id> critical-ip-addr <ip_address>
```

The **<vr_id>** parameter represents the virtual router being configured. The **<ip_address>** parameter represents the IP address to be used.

The **ip vrrp critical-ip-addr** command is executed in the Interface Configuration mode.

ip vrrp enable command

The **ip vrrp enable** command is used to enable the virtual router.

The syntax of the **ip vrrp enable** command is:

```
ip vrrp <vr_id> enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **ip vrrp enable** command is executed in the Interface Configuration mode.

no ip vrrp enable command

The **no ip vrrp enable** command is used to disable the virtual router.

The syntax of the **no ip vrrp enable** command is:

```
no ip vrrp <vr_id> enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **no ip vrrp enable** command is executed in the Interface Configuration mode.

ip vrrp fast-adv command

The **ip vrrp fast-adv** command is used to enable the VRRP fast advertisement functionality.

The syntax of the **ip vrrp fast-adv** command is:

```
ip vrrp <vr_id> fast-adv enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **ip vrrp fast-adv** command is executed in the Interface Configuration mode.

no ip vrrp fast-adv command

The **no ip vrrp fast-adv** command is used to disable the VRRP fast advertisement functionality.

The syntax of the **no ip vrrp fast-adv** command is:

```
no ip vrrp <vr_id> fast-adv enable
```

The **<vr_id>** parameter represents the virtual router being configured.

The **no ip vrrp fast-adv** command is executed in the Interface Configuration mode.

ip vrrp fast-adv-int command

The **ip vrrp fast-adv-int** command is used to set the interval used in the VRRP fast advertisement functionality.

The syntax of the **ip vrrp fast-adv-int** command is:

```
ip vrrp <vr_id> fast-adv-int <interval>
```

The **<vr_id>** parameter represents the virtual router being configured. The **<interval>** parameter represents the fast advertisement interval. This is a value in milliseconds between 200 and 1000.

The **ip vrrp fast-adv-int** command is executed in the Interface Configuration mode.

ip vrrp holddown-timer command

The **ip vrrp holddown-timer** command is used to set the VRRP holddown timer.

The syntax of the **ip vrrp holddown timer** command is:

```
ip vrrp <vr_id> holddown-timer <timer_value>
```

The **<vr_id>** parameter represents the virtual router being configured. The **<timer_value>** parameter represents the holddown timer value. This is a value in seconds between 0 and 21600.

The **ip vrrp holddown-timer** command is executed in the Interface Configuration mode.

ip vrrp priority command

The **ip vrrp priority** command is used to assign a priority to a virtual router.

The syntax of the **ip vrrp priority** command is:

```
ip vrrp <vr_id> priority <priority_value>
```

The **<vr_id>** parameter represents the virtual router being configured. The **<priority_value>** parameter represents the priority assigned to the virtual router. This is a value between 1 and 255.

The **ip vrrp priority** command is executed in the Interface Configuration mode.

show ip vrrp command

The **show ip vrrp** command is used to display VRRP configuration information and statistics.

The syntax of the **show ip vrrp** command is:

```
show ip vrrp [address] [interface]
```

Use either the **address** key word to display address-related VRRP information or **interface** to display interface-related VRRP information. Using neither displays basic global configuration information.

The command is executed in the Global Configuration mode.

Equal Cost MultiPath (ECMP) commands

The Equal Cost MultiPath (ECMP) feature allows routers to determine equal cost paths to the same destination prefix. The multiple paths can be used for load sharing of traffic and allows faster convergence to other active paths in case of network failure. This section describes the CLI commands used to configure ECMP on the switch.

> ***Note:*** ECMP is only supported on the Nortel Ethernet Routing Switch 5520 and 5530. ECMP will work in a mixed stack but will not run on any Nortel Ethernet Routing Switch 5510 units in the stack.

rip maximum-path command

The **rip maximum-path** command is used to configure the number of ECMP paths allotted for the Routing Information Protocol (RIP).

The syntax of the **rip maximum-path** command is:

```
rip maximum-path <path_count>
```

The **<path_count>** parameter represents the number of ECMP paths allotted. This is a value between 1 and 4. The default is 1.

The **rip maximum-path** command is executed in the Global Configuration mode.

ospf maximum-path command

The **ospf maximum-path** command is used to configure the number of ECMP paths allotted for the Open Shortest Path First (OSPF) protocol.

The syntax of the **ospf maximum-path** command is:

```
ospf maximum-path <path_count>
```

The **<path_count>** parameter represents the number of ECMP paths allotted. This is a value between 1 and 4. The default is 1.

The **ospf maximum-path** command is executed in the Global Configuration mode.

maximum-path command

The **maximum-path** command is used to configure the number of ECMP paths allotted to static routes.

The syntax of the **maximum-path** command is:

```
maximum-path <path_count>
```

The **<path_count>** parameter represents the number of ECMP paths allotted. This is a value between 1 and 4. The default is 1.

The **maximum-path** command is executed in the Global Configuration mode.

show ecmp command

The **show ecmp** command is used to display ECMP path information.

The syntax of the **show ecmp** command is:

```
show ecmp
```

The **show ecmp** command is executed in the User EXEC Configuration mode.

Brouter port commands

A brouter port is a single-port VLAN that can route IP packets as well as bridge all non-routable traffic. The following section describes the CLI commands used to configure and manage brouter ports on the Nortel Ethernet Routing Switch 5500 Series.

brouter command

The **brouter** command is used to create and manage a brouter port on the switch.

The syntax of the **brouter** command is:

```
brouter [port <brouter_port>] vlan <vid> subnet
<ip_address/mask> [routing enable]
```

The following table describes the parameters of this command.

brouter parameters

Parameter	Description
<brouter_port>	The brouter port. When creating a brouter this is the port to be used for the new brouter. When modifying a brouter this is the port of the existing brouter to modify.
<vid>	The VLAN ID of the brouter. When creating a new brouter port, this is the VLAN ID assigned to the brouter port.
<ip_address/mask>	The IP address and subnet mask of the brouter. When creating a new brouter, this is the IP address and subnet mask assigned. When modifying a brouter port, this is the new IP address and subnet mask to assign to the port. The subnet mask portion is expressed as a value between 0 and 32.

The **brouter** command is executed in the FastEthernet IEEE 802.3 Interface Configuration mode.

no brouter command

The **no brouter** command is used to disable or remove a brouter from the switch.

The syntax of the **no brouter** command is:

```
no brouter [port <brouter_port>] [routing enable]
```

The **<brouter_port>** parameter represents the brouter port to disable or remove from the switch.

The **no brouter** command is executed in the FastEthernet IEEE 802.3 Interface Configuration mode.

show brouter command

The **show brouter** command is used to display information about the brouter configuration on the switch.

The syntax of the **show brouter** command is:

```
show brouter [port <brouter_port>]
```

Usage of the optional **port <brouter_port>** port narrows the scope the command to the specified port. Omission of this parameter displays all ports.

The **show brouter** command is executed in the User EXEC mode.

UDP broadcast forwarding commands

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address. This section outlines the CLI commands used to configure and manage UDP broadcast forwarding on the switch.

ip forward-protocol udp command

The **ip forward-protocol udp** command is used to configure and manage UDP broadcast forwarding on the switch.

The syntax of the **ip forward-protocol udp** command is:

```
ip forward-protocol udp [<forwarding_port>
<protocol_name>] [portfwdlist <forward_list> <udp_port>
<destination_ip_address> name <list_name>]
```

The following table outlines the parameters of this command.

ip forward-protocol udp parameters

Parameter	Description
<forwarding_port>	The port on which the UDP protocol operates.
<protocol_name>	The name of the UDP protocol to be forwarded.
<forward_list>	A list of ports to which the UDP protocol will be forwarded.
<udp_port>	The UDP port on which the forwarding originates.
<destination_ip_address>	The destination IP address of the UDP forwarding.
<list_name>	The name of the forwarding list being created.

The **ip forward-protocol udp** command is executed in the Global Configuration mode.

clear ip forward-protocol udp counters command

The **clear ip forward-protocol udp counters** command clears the UDP broadcast counters on each interface.

TIP: Stacking - the **clear ip forward-protocol udp counters** command is executed only on the base unit in a stack.

The syntax for the **clear ip forward-protocol udp counters** command is:

```
clear ip forward-protocol udp counters <1-4094>
```

where the parameter <1-4094> specifies the VLAN ID.

The **clear ip forward-protocol udp counters** command is executed in the Configuration mode.

ip forward-iprotocol udp command (interface mode)

The **ip forward-protocol udp command** command, in interface mode, is used to attach and configure UDP broadcast forwarding lists on VLAN interfaces (only one list can be attached to a VLAN interface at a time).

The syntax of the **ip forward-protocol udp command (interface mode)** command is:

```
ip forward-protocol udp [vlan <vlan_id> portfwdlist
<forward_list> broadcastmask <bcast_mask> maxttl <max_ttl>]
```

The following table outlines the parameters of this command:

ip forward-protocol udp (interface mode) parameters

Parameter	Description
<vlan_id>	The VLAN ID of the interface on which the UDP forwarding list will be attached.
<forward_list>	The ID of the UDP forwarding list which will be attached to the selected VLAN interface.
<bcast_mask>	The 32 bit mask which will be used by the selected VLAN interface to take forwarding decisions based on the destination IP address of the incoming UDP broadcast traffic.
<max_ttl>	The TTL value which will be inserted in the IP headers of the forwarded UDP packets coming out of the selected VLAN interface.

The **ip forward-protocol udp command (interface mode)** command is executed in the Interface Configuration mode.

DHCP relay commands

This section covers the commands that are used to configure and manage DHCP on the Nortel Ethernet Routing Switch 5500 Series, both globally on the switch and on each VLAN.

Setting DHCP

To set DHCP, perform the following procedure:

Step	Action
1	Enable DHCP globally.
2	Set a VLAN IP as the DHCP agent and a Server IP as the DHCP server, to configure an ip dhcp-relay forwarding path.
3	Set the mode for each DHCP forwarding path.
4	Enable DHCP for the specific VLAN.
5	Enable the DHCP broadcast message for the specific VLAN.

—End—

ip dhcp-relay command

The **`ip dhcp-relay`** command is used to enable DHCP relay. DHCP relay is enabled by default.

The syntax for this command is:

```
ip dhcp-relay
```

This command is executed in the Global Configuration command mode.

This command has no parameters.

no ip dhcp-relay command

The no **`ip dhcp-relay`** command is used to disable DHCP relay.

The syntax for this command is:

```
no ip dhcp-relay
```

This command is executed in the Global Configuration command mode.

This command has no parameters.

show ip dhcp-relay counters command

The **show ip dhcp-relay counters** command displays the current DHCP relay counters configuration globally on the Nortel Ethernet Routing Switch 5500 Series. This includes the number of requests and the number of replies.

The syntax for the **show ip dhcp-relay counters** command is:

```
show ip dhcp-relay counters
```

The **show ip dhcp-relay counters** command is executed in the User EXEC command mode.

ip dhcp-relay clear-counters

The **ip dhcp-relay clear-counters** command clears the counters for an interface.

The syntax for this command is:

```
ip dhcp-relay clear-counters
```

This command is executed in the Interface Configuration command mode while editing a VLAN only.

This command has no parameters.

show ip dhcp-relay fwd-path command

The **show ip dhcp-relay fwd-path** command displays the current DHCP relay forward path configuration globally on the Nortel Ethernet Routing Switch 5500 Series which includes the interface, the server, the state (enabled or disabled), and the mode.

The syntax for the **show ip dhcp-relay fwd-path** command is:

```
show ip dhcp-relay fwd-path
```

The **show ip dhcp-relay fwd-path** command is executed in the User EXEC command mode.

ip dhcp-relay fwd-path command

The **ip dhcp-relay fwd-path** command sets the mode for the specific forwarding path DHCP relay settings globally on the Nortel Ethernet Routing Switch 5500 Series.

The syntax for the **ip dhcp-relay fwd-path** command is:

```
ip dhcp-relay fwd-path <A.B.C.D> <O.P.Q.R>
```

The following table outlines the parameters for this command.

ip dhcp-relay fwd-path parameters

Parameter	Description
<A.B.C.D>	Enter the IP address of the DHCP agent on the forwarding path to be configured.
<O.P.Q.R>	Enter the IP address of the DHCP server on the forwarding path to be configured.

The **ip dhcp-relay fwd-path** command is executed in the Global Configuration command mode.

The DHCP relay feature is enabled by default, and the default mode is BootP-DHCP.

ip dhcp-relay fwd-path enable command

The **ip dhcp-relay fwd-path enable** command enables the specific DHCP forwarding path globally on the Nortel Ethernet Routing Switch 5500 Series.

The syntax for the **ip dhcp-relay fwd-path enable** command is:

```
ip dhcp-relay fwd-path <A.B.C.D> <O.P.Q.R> enable
```

The following table describes the parameters for this command.

ip dhcp-relay fwd-path enable parameters

Parameter	Description
<A.B.C.D>	Enter the IP address of the DHCP agent on the forwarding path to be enabled.
<O.P.Q.R>	Enter the IP address of the DHCP server on the forwarding path to be enabled.

The **ip dhcp-relay fwd-path enable** command is executed in the Global Configuration command mode.

The DHCP feature is enabled by default.

ip dhcp-relay fwd-path disable command

The **ip dhcp-relay fwd-path disable** command disables the specific DHCP forwarding path globally on the Nortel Ethernet Routing Switch 5500 Series.

The syntax for the **ip dhcp-relay fwd-path disable** command is:

```
ip dhcp-relay fwd-path <A.B.C.D> <O.P.Q.R> disable
```

The following table describes the parameters for this command.

ip dhcp-relay fwd-path disable parameters

Parameter	Description
<A.B.C.D>	Enter the IP address of the DHCP agent on the forwarding path to be disabled.
<O.P.Q.R>	Enter the IP address of the DHCP server on the forwarding path to be disabled.

The **ip dhcp-relay fwd-path disable** command is executed in the Global Configuration command mode.

The DHCP relay feature is enabled by default.

no ip dhcp-relay fwd-path command

The **no ip dhcp-relay fwd-path** command removes the specified DHCP forwarding path globally on the Nortel Ethernet Routing Switch 5500 Series.

The syntax for the **no ip dhcp-relay fwd-path** command is:

```
no ip dhcp-relay fwd-path <A.B.C.D> <O.P.Q.R>
```

The following table outlines the parameters for this command.

no ip dhcp-relay fwd-path parameters

Parameter	Description
<A.B.C.D>	Enter the IP address of the DHCP agent on the forwarding path to be removed.
<O.P.Q.R>	Enter the IP address of the DHCP server on the forwarding path to be removed.

The **no ip dhcp-relay fwd-path** command is executed in the Global Configuration command mode.

show vlan dhcp-relay command

The **show vlan dhcp-relay** command displays the current DHCP relay forward path configuration for each VLAN on the Nortel Ethernet Routing Switch 5500 Series.

The syntax for the **show vlan dhcp-relay** command is:

```
show vlan dhcp-relay [<1-4094>]
```

Substitute **<1-4094>** above with the VLAN ID of the VLAN to be displayed.

The **show vlan dhcp-relay** command is executed in the User EXEC command mode.

ip dhcp-relay command

The **ip dhcp-relay** command allows configures DHCP relay settings on a VLAN.

The syntax for the **ip dhcp-relay** command is:

```
ip dhcp-relay [min-sec <0-65535>] [mode {bootp | dhcp |
bootp_dhcp}]
```

The following table outlines the parameters for this command.

ip dhcp-relay parameters

Parameter	Description
min-sec <0-65535>	Enter the minimum number of seconds to wait between receiving the DHCP packet and forwarding it to the destination device. The default is 0.
mode {bootp | dhcp | bootp_dhcp}	Enter the type of DHCP packets this VLAN supports: • bootp - Supports BootP only • dhcp - Supports DHCP only • bootp_dhcp - Supports both BootP and DHCP

The **ip dhcp-relay** command is executed in the Interface Configuration command mode.

no ip dhcp-relay command

The **no ip dhcp-relay** command disables DHCP relay on a VLAN.

The syntax for the **no ip dhcp-relay** command is:

```
no ip dhcp-relay
```

The **no ip dhcp-relay** command is executed in the Interface Configuration command mode.

ip dhcp-relay broadcast command

The **ip dhcp-relay broadcast** command enables DHCP relay broadcast on a VLAN.

The syntax for the **ip dhcp-relay broadcast** command is:

ip dhcp-relay broadcast

The **ip dhcp-relay broadcast** command is executed in the Interface Configuration command mode.

no ip dhcp-relay broadcast command

The **no ip dhcp-relay broadcast** command disables DHCP relay broadcast on a VLAN.

The syntax for the **no ip dhcp-relay broadcast** command is:

no ip dhcp-relay broadcast

The **no ip dhcp-relay broadcast** command is executed in the Interface Configuration command mode.

IP routing configuration examples

This section provides configuration examples for common IP routing tasks using the Command Line Interface (CLI). For conceptual information about the IP routing topics covered in this section, refer to "An Introduction to IP Routing Protocols" (page 13).

> ***Note:*** In many of the following configuration examples, a brouter port is used to create a connection to the network core. This practice does not imply that a brouter port is the only means through which a core connection can be established. The use of a brouter port is only one of many ways to create such a connection.

Address Resolution Protocol (ARP) configuration

The Nortel Ethernet Routing Switch 5500 Series provides the following Address Resolution Protocol (ARP) features:

- Default ARP aging
- Static ARP entries
- Proxy ARP

Static ARP entries can be used to solve the following instances encountered on many networks:

- To communicate with a device that does not respond to an ARP request.
- To prevent an existing ARP entry from aging out.

When a static ARP entry is configured, both the IP address and MAC address of a device is assigned to a physical port. This includes the VLAN number if the physical port is associated with a VLAN.

This section contains the following topics:

Changing the default ARP aging time

The default ARP aging time value is set for 360 minutes. To change this default aging time use the **ip arp timeout** command. This command has the following syntax:

```
ip arp timeout <minutes>
```

The **<minutes>** parameter represents the number of minutes to set for the new timeout setting. This is a value in the range of 5 to 360.

The following is an example of setting a new default aging time:

```
5530-24TFD(config)# ip arp timeout 180
```

The new setting can be confirmed by using the **show ip routing** command.

Adding a static ARP entry to a VLAN

To add a static ARP entry to a VLAN, use the **ip arp** command. This command has the following syntax:

```
ip arp ip <ip_address> mac <mac_address> port <port_number>
vid <vid_number>
```

The following table outlines the parameters of this command

ip arp parameters

Parameter	Description
ip_address	The IP address of the entry.
mac_address	The MAC address of the entry.
port_number	The slot/port number of the brouter port.
vid_number	The VLAN ID of the entry.

The following is an example of adding a static ARP entry to a VLAN:

```
5530-24TFD(config)# ip arp 10.1.1.23 00:00:11:43:54:23 1/48
vid 1
```

Adding a static ARP entry to a brouter port

To add a static ARP entry to a brouter port, use the **ip arp** command. This command has the following syntax:

```
ip arp ip <ip_address> mac <mac_address> port <port_number>
vid <vid_number>
```

The following table outlines the parameters of this command

ip arp parameters

Parameter	Description
ip_address	The IP address of the entry.
mac_address	The MAC address of the entry.
port_number	The slot/port number of the brouter port.
vid_number	The VLAN ID of the entry.

The following is an example of adding a static ARP entry to a brouter port:

```
5530-24TFD(config)# ip arp 172.2.2.13 00:00:98:22:33:44 1/46
vid 1
```

Deleting a static ARP entry

To delete a static ARP entry, use the **no ip arp** command. This command has the following syntax:

```
no ip arp ip <ip_address>
```

The **<ip_address>** parameter represents the IP address of the entry to delete.

The following is an example of deleting a static ARP entry:

```
5530-24TFD(config)# no ip arp 172.2.2.13
```

Note: Deleting a static ARP entry is applicable to both VLANs and brouter ports.

Routing Information Protocol (RIP) configuration

This section provides examples of the common RIP configuration tasks and includes the CLI commands used to create the configuration.

RIP configuration tasks

RIP is configured on a VLAN or brouter port basis. This section presents the steps in RIP configuration and accompanying command syntax examples.

To configure RIP on an interface, perform the following steps:

Note: The command examples below demonstrate the configuration of RIP on a VLAN.

Step	Action

1 Configure the interface, assign an IP address and add ports.

```
5530-24TFD# enable
5530-24TFD#config terminal
5530-24TFD(config)# vlan create 51 name "VLAN-51" type
port
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip address 10.10.1.1
255.255.255.0
5530-24TFD(config-if)# exit
5530-24TFD(config)# vlan members add 51 8-9
```

2 Enable RIP.

Note: Perform one of the following command sequences to enable RIP.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip enable
```

OR

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# router rip
5530-24TFD(config-router)# network 10.10.1.1
```

3 Disable Supply RIP Updates, if required.

```
5530-24TFD#  enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip supply disable
```

4 Disable Listen for RIP Updates, if required.

```
5530-24TFD# enable
5530-24TFD#config terminal
5530-24TFD(config)#interface vlan 51
5530-24TFD(config-if)# ip rip listen disable
```

5 Enable Default Route Supply, if a default route exists in the route table.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
```

```
5530-24TFD(config-if)# ip rip default-supply enable
```

6 Enable Default Route Listen to add a default route to the route table, if advertised from another router.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip default-listen enable
```

7 Add the In or Out Route Policy.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip out-policy map1
```

8 Enable Triggered Updates, if required.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip triggered enable
```

9 Configure the cost of the link by entering a value of 1 to 15; where 1 is the default.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip cost 2
```

10 Configure send mode parameters.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# router rip enable
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip send version rip2
```

11 Configure receive mode parameters.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# router rip enable
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip receive version rip2
```

12 Enable poison reverse.

Note: RIP Split Horizon is enabled by default. By setting the Poison parameter to true, Poison Reverse is enabled. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16.

Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.

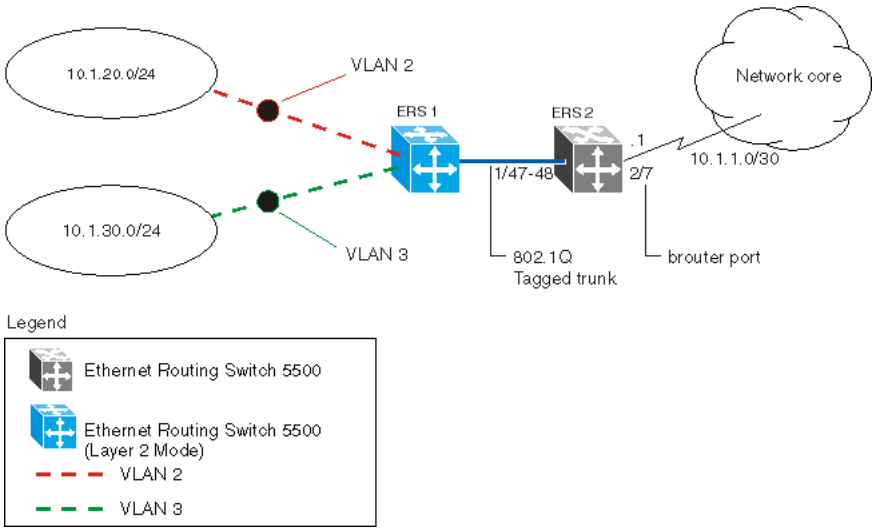
```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 51
5530-24TFD(config-if)# ip rip
5530-24TFD(config-if)# ip rip poison enable
```

—End—

Configuring RIP

This section describes the set up of a basic RIP configuration between two Nortel Ethernet Routing Switch 5500 Series routers. As illustrated in the following diagram, router ERS2 is configured between router ERS1 and the edge of the network core. Two VLANs (VLAN 2 and 3) are associated with ERS1.

RIP configuration example



For the purposes of this example:

- ERS1 is an edge switch with two configured VLANs, VLAN 2 and 3. It is connected to aggregation switch ERS2 on ports 1/47 and 1/48.
- Port 2/7 of ERS2 is configured as a brouter port with RIP to connect to the network core.

Use the following procedure to configure router ERS 2 and reproduce the illustrated RIP configuration:

Step	Action

1 Configure tagging on ports 1/47 and 1/48. Tagging is required to support multiple VLANs on the same interface.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# vlan ports 1/47-48 tagging tagAll
```

2 Configure ERS2 for VLAN 2 access.

a. Create a port-based VLAN (VLAN 2) using spanning tree group 1 and include ports 1/47 and 1/48 in VLAN 2.

```
5530-24TFD(config)# vlan create 2 name "VLAN-2" type
port
5530-24TFD(config)# vlan member add 2 port 1/47-48
```

b. Assign the IP address 10.1.20.2/24 to VLAN 2.

```
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip address 10.1.20.2
255.255.255.0
```

c. Enable RIP for VLAN 2 and disable RIP supply and listen. RIP supply and listen are not required because no router is attached to VLAN 2.

```
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip rip enable
5530-24TFD(config-if)# ip rip supply disable
5530-24TFD(config-if)# ip rip listen disable
```

3 Configure ERS2 for VLAN 3 access.

a. Create a port-based VLAN (VLAN 3) using spanning tree group 1 and include ports 1/47 and 1/48 in VLAN3.

```
5530-24TFD(config)# vlan create 3 name "VLAN-3" type
port
5530-24TFD(config)# vlan member add 3 port 1/47-48
```

b. Assign the IP address 10.1.30.2/24 to VLAN 3.

```
5530-24TFD(config)# interface vlan 3
5530-24TFD(config-if)# ip address 10.1.30.2
255.255.255.0
```

c. Enable RIP for VLAN 3 and disable RIP supply and listen. RIP supply and listen are not required because no router is attached to VLAN 3.

```
5530-24TFD(config)# interface vlan 3
5530-24TFD(config-if)# ip rip enable
5530-24TFD(config-if)# ip rip supply disable
```

```
5530-24TFD(config-if)#ip rip listen disable
```

4 Configure brouter port 2/7 on ERS2.

a. Assign the IP address 10.1.1.1/30 to port 2/7 using brouter VLAN 2090.

```
5530-24TFD(config)# interface FastEthernet 2/7
5530-24TFD(config-if)# brouter vlan 2090 subnet
10.1.1.1/30
```

Note: Usage of the **brouter** command above requires the usage of Variable Length Subnetting. Usage of a dotted decimal subnet mask is not allowed.

b. Enable RIP on the interface.

```
5530-24TFD(config)# interface FastEthernet 2/7
5530-24TFD(config-if)# ip rip enable
```

5 Enable IP routing and RIP globally.

```
5530-24TFD(config)# ip routing
5530-24TFD(config)# router rip enable
```

—End—

A list of the commands used to create this configuration can be displayed using the **show running-config** command. Using this command on ERS2 would list the following commands:

```
! *** VLAN *** !
vlan igmp unknown-mcast-no-flood disable
vlan configcontrol strict
auto-pvid
vlan name 1 "VLAN #1"
vlan create 2 name "VLAN-2" type port
vlan create 3 name "VLAN-3" type port
vlan members 2 1/47-48
vlan members 3 1/47-48
! *** RIP ***  !
router rip
router rip enable
timers basic holddown 120
timers basic timeout 180 update 30 default-metric 8
network 10.1.20.2
network 10.1.30.2
network 10.1.1.1
interface vlan 2
no ip rip listen enable
no ip rip supply enable
```

```
interface vlan 3
no ip rip listen enable
no ip rip supply enable
! *** Brouter Port *** !
interface fastEthernet ALL
brouter port 2/7 vlan 3 subnet 10.1.1.1/30
```

The following commands can be used to confirm the configuration of RIP parameters:

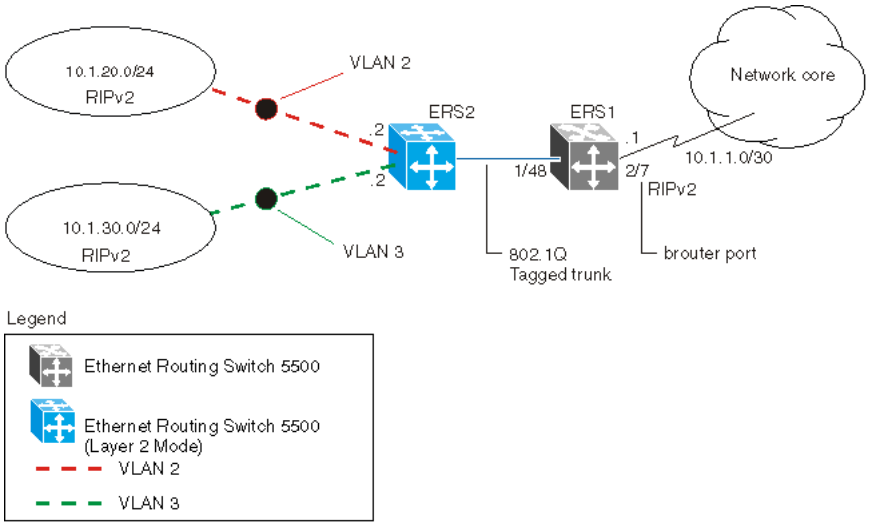
Command	Description
`show vlan`	This command is used to display information about the currently configured switch VLANs.
`show vlan ip`	This command is used to display IP address information about VLANs that have been assigned addresses on the switch.
`show ip rip`	This command displays information on the global switch RIP configuration.
`show ip route`	This command displays the switch routing table.
`show ip rip interface`	This command displays information about the RIP interfaces present on the switch.

Configuring RIP version 2

When RIP is enabled on an interface, it operates by default in **rip1compatible** send mode and **rip1orRip2** receive mode. Depending on configuration requirements, the Nortel Ethernet Routing Switch 5500 Series can be configured to operate using RIP version 1 or 2. The configuration illustrated below demonstrates a Nortel Ethernet Routing Switch 5500 Series switch that has been configured to operate use RIP version 2 only.

Note: This example builds on the previous RIP configuration.

RIPv2 configuration example



Use the following procedure to configure ERS2 to add RIP version 2 to VLAN 2, VLAN 3, and the brouter port:

Step	Action

1 Configure RIP version 2 on VLAN 2. Enable RIP version 2 mode on the IP address used for VLAN 2.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# router rip enable
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip rip send version rip2
5530-24TFD(config-if)# ip rip receive version rip2
```

2 Configure RIP version 2 on VLAN 3. Enable RIP version 2 mode on the IP address used for VLAN 3.

```
5530-24TFD# enable
5530-24TFD# config terminal
5530-24TFD(config)# router rip enable
5530-24TFD(config)# interface vlan 3
5530-24TFD(config-if)# ip rip send version rip2
5530-24TFD(config)# router rip enable
5530-24TFD(config)# interface vlan 3
5530-24TFD(config-if)# ip rip receive version rip2
```

3 Configure RIP version 2 on the brouter port. Enable RIP version 2 mode on the IP address used for the brouter port.

```
5530-24TFD(config)# interface FastEthernet 2/7
5530-24TFD(config-if)# ip rip enable
5530-24TFD(config-if)# ip rip send version rip2
```

```
5530-24TFD(config-if)# ip rip receive version rip2
```

—End—

Using RIP accept policies

RIP accept policies are used on the Nortel Ethernet Routing Switch 5500 Series to selectively accept routes from RIP updates. If no policies are defined, the default behavior is applied. This default behavior is to add all learned routes to the route table. RIP accept policies are used to:

- Listen to RIP updates only from certain gateways.
- Listen only for specific networks.
- Assign a specific mask to be included with a network in the routing table (such as a network summary).

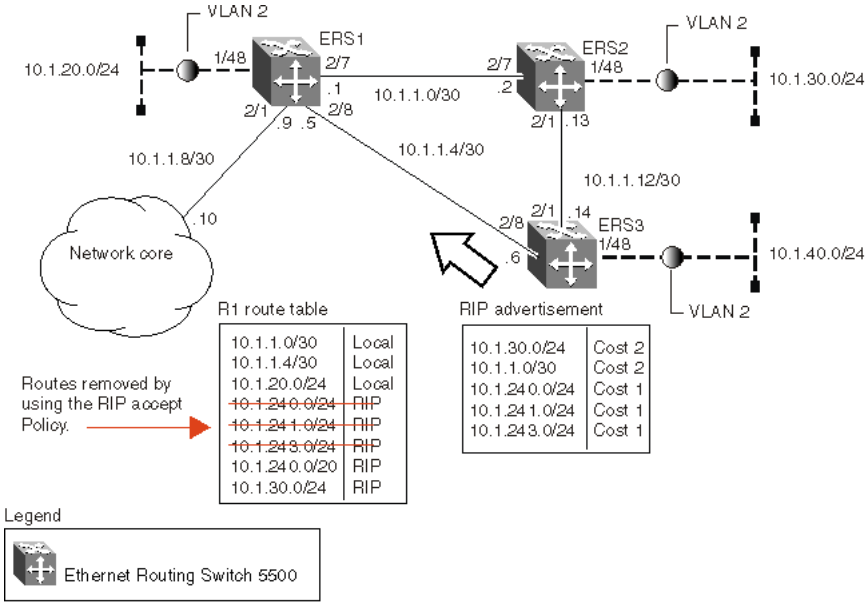
In the configuration illustrated below, the Nortel Ethernet Routing Switch 5500 Series (ERS1) is configured with a RIP accept policy. This creates a single route directed to ERS3 for all networks configured on it. The accept policy accepts any network from 10.1.240.0 to 10.1.255.0, and creates a single entry in the routing table on ERS1.

A summary route is calculated by comparing the common bits in the address range to derive the summary address. For example, if the range of IP addresses is from 10.1.240.0 to 10.1.255.0:

1. Determine the third octet of the first address: 10.1.240.0 = 1111 0000.
2. Determine the third octet of the ending address: 10.1.255.0 = 1111 1111.
3. Extract the common bits: 240 = 1111 0000 255 = 1111 1111 1111 = 20 bit mask.

Therefore, the network address to use for this example is 10.1.240.0/20

Accept policy configuration



Use the following steps to recreate the above configuration example:

Step	Action
1	Configure the IP prefix list on ERS1. Create a prefix list named **Prefix_1** with an IP range from 10.1.240.0 to 10.1.255.0. **5530-24TFD(config)# ip prefix-list Prefix_1 10.1.240.0/20 ge 20 le 32**
2	Configure the route policy named **rip_pol_1** with match criteria using the IP prefix configured in step 1. This injects one route of 10.1.240.0/20 into the route table. **5530-24TFD(config)# route-map rip_pol_1 1** **5530-24TFD(config)# route-map rip_pol_1 1 enable** **5530-24TFD(config)# route-map rip_pol_1 permit 1 enable** **5530-24TFD(config)# route-map rip_pol_1 permit 1 match network Prefix_1** **5530-24TFD(config)# route-map rip_pol_1 permit 1 set-injectlist Prefix_1**
3	Add the route policy created in step 2 to both RIP core ports. **5530-24TFD(config)# interface FastEthernet 2/7** **5530-24TFD(config-if)# brouter vlan 2090 subnet 10.1.1.1/30** **5530-24TFD(config-if)# ip rip enable** **5530-24TFD(config-if)# ip rip in-policy rip_pol_1**

```
5530-24TFD(config)# interface FastEthernet 2/8
5530-24TFD(config-if)# brouter vlan 2091 subnet
10.1.1.5/30
5530-24TFD(config-if)# ip rip enable
5530-24TFD(config-if)# ip rip in-policy rip_pol_1
```

—End—

The **show running-config** command is used to display the current configuration of a switch. Using this command on the above configuration would yield the following results:

```
rip_pol_1
! *** Route Policies *** !
ip prefix-list Prefix_1 10.1.240.0/20 ge 20 le 32
route-map rip_pol_1
route-map rip_pol_1 1 enable
no route-map rip_pol_1 1 match interface
route-map rip_pol_1  1 match metric 0
route-map rip_pol_1  1 match network Prefix_1
no route-map rip_pol_1 1 match next-hop
route-map rip_pol_1  1 match route-type any
no route-map rip_pol_1 match route-source
route-map rip_pol_1 1 set injectlist Prefix_1
route-map rip_pol_1 set mask  0.0.0.0
route-map rip_pol_1 set metric 0
route-map rip_pol_1 set nssa-pbit enable
route-map rip_pol_1 set ip-preference 0
! *** Brouter Port *** !
interface fastEthernet ALL
brouter port 2/7
vlan 2090 subnet 10.1.1.1/30
ip rip in-policy rip_pol_1
brouter port 2/8 vlan 2091 subnet 10.1.1.5/30
ip rip in-policy rip_pol_1
```

Using RIP announce policies

In the previous configuration example, a RIP accept policy is used on ERS1 to insert a single route into its route table for all networks from ERS3. Instead of using an accept policy on ERS1, a RIP announce policy on ERS3 could be used to announce a single route to both ERS1 and ERS2 for the local network range.

To configure the RIP announce policy on ERS3, use the following configuration steps:

Step	Action
1	Configure the IP prefix list on ERS3 named **Prefix_1** with the IP address 10.1.240.0. `5530-24TFD(config)# ip prefix-list Prefix_1 10.1.240.0/20 ge 20 le 32`

2	Configure the route policy named **Policy_Rip** with match criteria using the IP prefix configured in step 1.
	`5530-24TFD(config)# route-map rip_pol_1 1`
	`5530-24TFD(config)# route-map rip_pol_1 1 enable`
	`5530-24TFD(config)# route-map rip_pol_1 permit 1 enable`
	`5530-24TFD(config)# route-map rip_pol_1 permit 1 set-injectlist Prefix_1`

3	Add the route policy created in step 2 to both RIP core ports.
	`5530-24TFD(config)# interface FastEthernet 2/1`
	`5530-24TFD(config-if)# brouter vlan 2091 subnet 10.1.1.14/30`
	`5530-24TFD(config-if)# ip rip enable`
	`5530-24TFD(config-if)# ip rip out-policy rip_pol_1`
	`5530-24TFD(config)# interface FastEthernet 2/8`
	`5530-24TFD(config-if)# brouter vlan 2090 subnet 10.1.1.6/30`
	`5530-24TFD(config-if)# ip rip enable`
	`5530-24TFD(config-if)# ip rip out-policy rip_pol_1`

—End—

To limit the advertising of routes using the announce policy from the routing table, a route policy should be created to deny the route. To configure the RIP announce policy with a limited announce policy on ERS3, use the following configuration steps:

Step	Action
1	Configure the IP prefix list named **Prefix_2** with the IP address 10.1.240.0. `5530-24TFD(config)# ip prefix-list Prefix_2 10.1.240.0/20 ge 20 le 20`
2	Configure the IP route policy named **rip_pol_2** with match criteria using the IP prefix configured in Step 1. `5530-24TFD(config)# route-map rip_pol_2 deny 1 enable match network Prefix_2`

```
5530-24TFD(config)# route-map rip_pol_2 1 match
network Prefix_2
```

3 Add the Route Policy created in step 2 to both RIP core ports.

```
5530-24TFD(config)# interface FastEthernet 2/1
5530-24TFD(config-if)# brouter vlan 2091
subnet 10.1.1.14/30
5530-24TFD(config-if)# ip rip enable
5530-24TFD(config-if)#ip rip out-policy rip_pol_2
5530-24TFD(config)# interface FastEthernet 2/8
5530-24TFD(config-if)# brouter vlan 2090
subnet 10.1.1.6/30
5530-24TFD(config-if)# ip rip enable
5530-24TFD(config-if)# ip rip out-policy rip_pol_2
```

—End—

Open Shortest Path First (OSPF) configuration

This section contains examples of common OSPF-related configuration tasks.

The Nortel Ethernet Routing Switch 5500 Series supports the following OSPF standards:

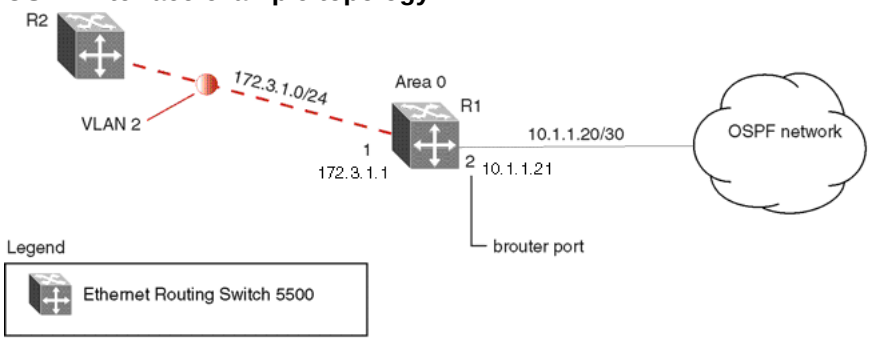
- RFC 2328 (OSPF version 2)
- RFC 1850 (OSPF Management Information Base)
- RFC 2178 (OSPF MD5 cryptographic authentication)

This section provides examples of the common OSPF configuration tasks and includes the CLI commands used to create the configuration.

configuring an IP OSPF interface

An OSPF interface can be configured on a brouter port or on a VLAN. The following section demonstrates the creation of the example OSPF interface illustrated below.

OSPF interface example topology



To create the OSPF interface illustrated above for router R1, follow this procedure:

Step	Action

1	Configure brouter port OSPF interface.
	
	Configure port 2 as a brouter port with VLAN ID of 2134 and enable OSPF on this interface.
	
	`5530-24TFD# config terminal`
	`5530-24TFD(config)# interface fast 2`
	`5530-24TFD(config-if)# brouter port 2 vlan 2134 subnet 10.1.1.21/30`
	`5530-24TFD(config-if)# router ospf`
	`5530-24TFD(config-router)# network 10.1.1.21`

2	Configure the VLAN OSPF interface.
	
	Create a port-based VLAN (VLAN 2) using spanning tree group 1, assign IP address 172.3.1.1 to VLAN 2 and enable OSPF on this interface.
	
	`5530-24TFD(config)# vlan create 2 type port`
	`5530-24TFD(config)# spanning-tree stp 1 add-vlan 2`
	`5530-24TFD(config)# vlan member add 2 1`
	`5530-24TFD(config)# interface vlan 2`
	`5530-24TFD(config-if)# ip address 172.3.1.1 255.255.255.0`
	`5530-24TFD(config-if)# router ospf`
	`5530-24TFD(config-router)# network 172.3.1.1`

3	Assign a router ID to the new interface and enable OSPF globally.
	
	`5530-24TFD(config)# router ospf`
	`5530-24TFD(config-router)# router-id 1.1.1.1`
	`5530-24TFD(config-router)# exit`
	`5530-24TFD(config)# router ospf enable`

—End—

OSPF security

The Nortel Ethernet Routing Switch 5500 Series implementation of OSPF includes security mechanisms to prevent the OSPF routing domain from being attacked by unauthorized routers. These security mechanisms prevent a malicious person from joining an OSPF domain and advertising false information in its OSPF link state advertisements. Likewise, the security prevents a misconfigured router from joining an OSPF domain. Currently there are two security mechanisms supported: simple password security and Message Digest 5 (MD5) security.

Simple password mechanism The simple password security mechanism transmits a text password in the OSPF headers. Only routers that contain the same authentication ID in their OSPF headers can communicate with each other.

> ***Note:*** Nortel recommends not using this security mechanism because the password is stored in plain text and can be read from the configuration file or from the OSPF packet.

To configure this authentication type on an OSPF interface of VLAN 2 using the password **test1234**, use the following commands:

```
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip ospf authentication-type simple
5530-24TFD(config-if)# ip ospf authentication-key test1234
```

Message Digest 5 The Message Digest 5 (MD5) mechanism provides 128-bit encrypted authentication based on the RFC 1321 standard. MD5 authentication for OSPF security, makes it very hard for a malicious user to compute or extrapolate the decrypting codes from the OSPF packets. Basically, each OSPF packet has a message digest appended to it, which needs to be matched between sending and receiving routers. The message digest is calculated on either side, based on the MD5 Key and any padding, then compared for a match. If the message digest does not meet the match criteria, the packet is rejected.

Each OSPF interface supports up to 2 keys, identifiable by key ID, to facilitate a smooth key transition during the rollover process. Only the selected primary key is used to encrypt the OSPF transmit packets.

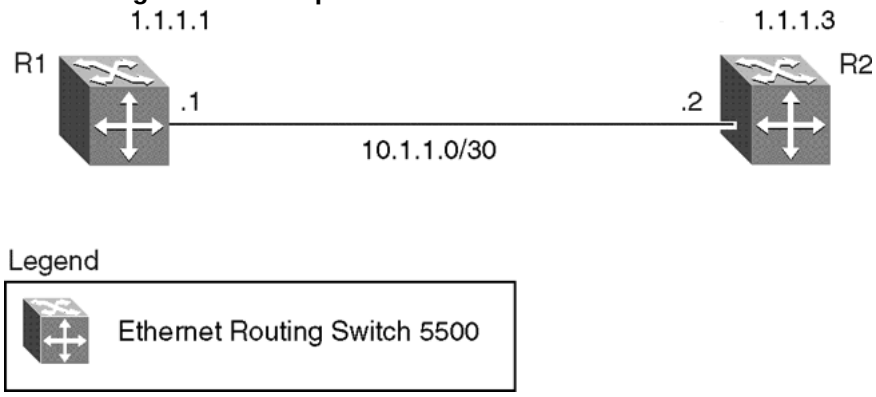
The process of key change is as follows:

> ***Note:*** Assume that all routers already use the same key for authentication and a new key is required.

1. Add the second key to all routers. The routers will continue to send OSPF packets encrypted with the old key.
2. Activate the second key on all routers by setting it as the primary key. Routers will send OSPF packets encrypted with the new key while still accepting packets using the old key. This is necessary as some routers will not have activated the new key.
3. Remove the old key when all routers activate the new key.

MD5 configuration example In the configuration example illustrated below, MD5 is configured between router R1 and R2.

MD5 configuration example



To replicate the above configuration example using the key ID 2 and key value **qwsdf89**, perform the following steps:

Step	Action

1	Configure MD5 authentication on R1.
	`5530-24TFD(config)# interface vlan 2`
	`5530-24TFD(config-if)# ip ospf message-digest-key 2 md5 qwsdf89`
	`5530-24TFD(config-if)# ip ospf primary-md5-key 2`
	`5530-24TFD(config-if)# ip ospf authentication-type message-digest`

2	Configure MD5 authentication on R2.
	`5530-24TFD(config)# interface vlan 2`
	`5530-24TFD(config-if)# ip ospf message-digest-key 2 md5 qwsdf89`
	`5530-24TFD(config-if)# ip ospf primary-md5-key 2`
	`5530-24TFD(config-if)# ip ospf authentication-type message-digest`

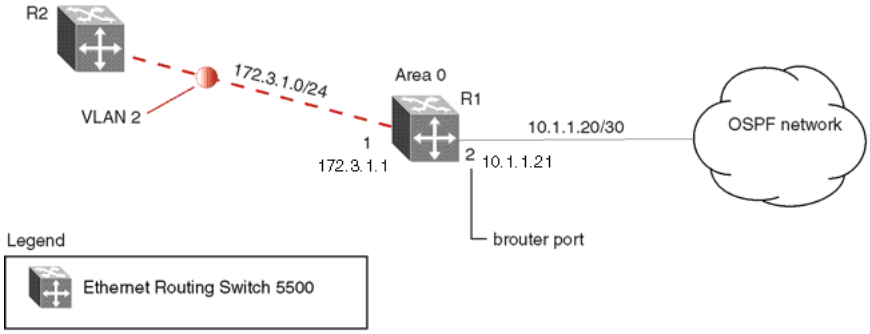
—End—

Configuring OSPF network types

OSPF network types were created to allow OSPF-neighboring between routers over different types of network infrastructures. With this feature, each interface can be configured to support the various network types.

In the example configuration illustrated below, VLAN 2 on Nortel Ethernet Routing Switch 5500 Series R1 is configured for OSPF with the interface type field value set as **passive**. Because VLAN 2 is set as **passive**, OSPF hello messages are not sent on this segment, although R1 continues to advertise this interface to the remaining OSPF network.

OSPF network example



To create the configuration illustrated above for router R1, use the following commands:

```
5530-24TFD(config)# vlan create 2 type port
5530-24TFD(config)# vlan mem add 2 1
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip address 172.3.1.1 255.255.255.0
5530-24TFD(config-if)# ip ospf network passive
```

The Nortel Ethernet Routing Switch 5500 Series supports the following types of networks:

- **Broadcast** - Automatically discovers every OSPF router on the network by sending OSPF hellos to the multicast group **AllSPFRouters** (224.0.0.5). Neighboring is automatic and requires no configuration. This interface type is typically used in an Ethernet environment.
- **Passive** - Allows interface network to be included in OSPF without generating LSAs or forming adjacencies. Typically used on an access network, or on an interface that is used for BGP peering. This also limits the amount of CPU cycles required to process the OSPF routing algorithm.

Configuring OSPF areas

In large networks with many routers and networks, the link state database (LSDB) and routing table can become very large. Large route tables and link state databases (LSDB) consume memory. The processing of link state advertisements results in more CPU cycles required to make forwarding decisions. To help reduce these undesired effects, an OSPF network can be divided into subdomains called areas. An area is made up of a number of OSPF routers that have the same area identification.

By dividing a network into multiple areas, a separate LSDB, consisting of router link state advertisements (LSA) and network LSAs are maintained for each area. Each router within an area maintains an LSDB only for the area to which it belongs. For example, the area router LSAs and network LSAs are not flooded beyond the area borders.

The impact of a topology change is localized to the area in which it occurs. The only exception to this is for the area border routers, which must maintain an LSDB for each area to which they belong. Changes in topology are advertised to the rest of the network by the area border routers by advertising summary LSAs.

A 32-bit Area ID, expressed in IP address format such as 0.0.0.0 for 0 identifies areas. Area 0 is also known as the backbone area and is responsible for distributing routing information to all other areas.

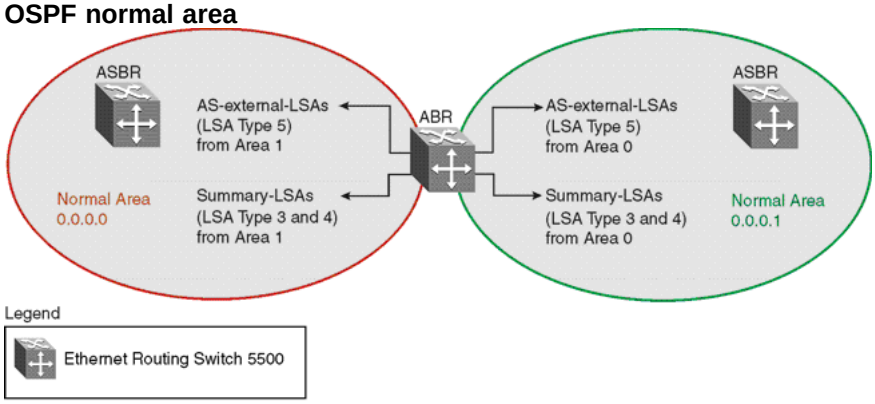
If multiple areas are used, they must all be attached to the backbone through an Area Border Router (ABR), which connects area 0.0.0.0 to the non-backbone areas.

Normal area A normal area is a collection of routers that use the same Area-ID that calculates inter-area and external routes through the use of the following link state advertisements:

- Summary LSAs
- ASBR-summary LSAs
- AS-external LSAs

As illustrated in the following figure, a normal area supports Area Border Routers (ABRs) and Autonomous System Border Routers (ASBRs).

OSPF normal area



The Nortel Ethernet Routing Switch 5500 Series automatically becomes an ABR when more than one area is configured for it and each area has at least one operational interface. To designate a router as an ASBR, use the **as-boundary-router enable** command.

```
5530-24TFD(config-router)# as-boundary-router enable
```

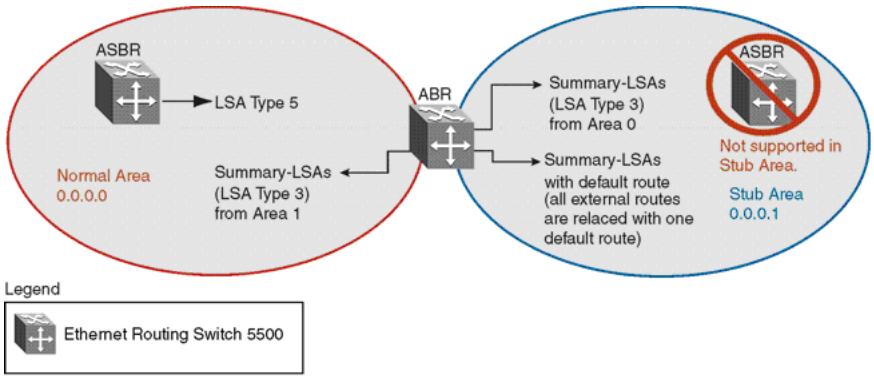
Stub and Not So Stubby areas Stub areas do not receive advertisements for external routes (AS-external LSAs, type 5) from an ABR, which reduces the size of the link state database. Instead, routing to external destinations from within a stub area is based on the default route that is originated by the stub area ABR (Summary LSA, type 3).

Import summary can be disabled on a stub area ABR to further prevent redistribution of summary routes from other areas into the stub area. In this case, the stub area ABR advertises only default routes into the stub area.

Note: Disabling import summaries is only allowed in the stub area.

As shown in the following figure, a stub area has only one ABR. All packets that are destined to be forwarded outside the stub area are routed to the stub areas border exit point, where the ABR first examines the packets and then forwarded to a destination.

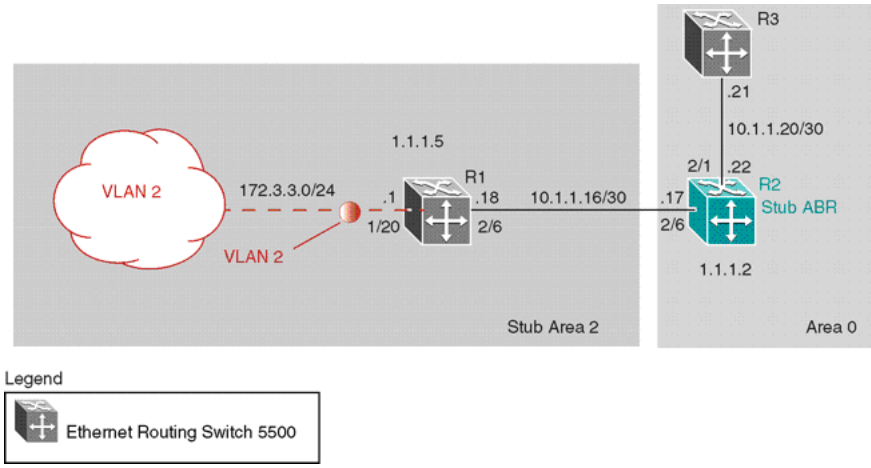
OSPF stub area



Note: Stub areas do not support ASBRs. In all routers attached to the stub area, the area must be configured as a stub area.

In the configuration example illustrated below, the Nortel Ethernet Routing Switch 5500 Series R1 is configured in Stub Area 2, and R2 is configured as a Stub ABR for Area 2.

OSPF stub area example



Note: AS-external LSAs are not flooded into a stub area. Instead, only one default route to external destinations is distributed into the stub area by the stub ABR router. The area default cost specifies the cost for advertising the default route into stub area by the ABR.

Use the procedure outlined below to perform the stub area configuration illustrated above:

Note: This example assumes that global IP routing has been enabled on the switch. Global IP routing is enabled on the switch in Global Configuration mode using the **`ip routing`** command.

Step	Action

1 Configure router R1.

a. Configure the OSPF interface on R1.

Configure port 2/6 as a brouter port in VLAN 100.

```
5530-24TFD(config)# interface fast 2/6
5530-24TFD(config-if)# brouter port 2/6 vlan 100
subnet 10.1.1.18/30
```

b. Configure VLAN 2 on R1.

Create VLAN 2 and assign an IP address to it.

```
5530-24TFD(config)# vlan create 2 type port
5530-24TFD(config)# vlan mem add 2 1/20
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip address 172.3.3.1
255.255.255.0
```

c. Enable OSPF on R1.

Configure R1 in stub area 2 with the Router-ID 1.1.1.5. Add the OSPF interfaces to area 2 and enable OSPF on these interfaces.

```
5530-24TFD(config-router)# router-id 1.1.1.5
5530-24TFD(config-router)# area 0.0.0.2 import
noexternal
5530-24TFD(config-router)# network 10.1.1.18 area
0.0.0.2
5530-24TFD(config-router)# network 172.3.3.1 area
0.0.0.2
5530-24TFD(config)# router ospf enable
```

2 Configure router R2.

a. Configure the OSPF interface on R2.

Configure port 2/6 as a brouter port in VLAN 100.

```
5530-24TFD(config)# interface fast 2/6
5530-24TFD(config-if)# brouter port 2/6 vlan 100
subnet 10.1.1.17/30
```

b. Configure the second OSPF interface on R2.

Configure port 2/1 as a brouter port in VLAN 300. Enable OSPF on this interface.

```
5530-24TFD(config)# interface fast 2/1
5530-24TFD(config-if)# brouter port 2/1 vlan 300
subnet 10.1.1.22/30
5530-24TFD(config-if)# ip ospf enable
```

c. Enable OSPF on R2.

Configure R2 in stub area 2 with an area default cost of 10. Disable import summary to prevent R2 from sending summary LSAs of area 0 into area 2. R2 will originate only summary LSA for default route into area 2. Note that, by default, OSPF interface 10.1.1.22 is placed into OSPF area 0.0.0.0. Because one additional area of 0.0.0.2 is added and OSPF interface 10.1.1.17 is added to area 0.0.0.2, R2 automatically becomes a stub ABR.

```
5530-24TFD(config-router)# router-id 1.1.1.2
5530-24TFD(config-router)# area 0.0.0.2 import
noexternal
5530-24TFD(config-router)# no area 0.0.0.2
import-summary enable
5530-24TFD(config-router)# area 0.0.0.2 default-cost
10
5530-24TFD(config-router)# network 10.1.1.17 area
0.0.0.2
5530-24TFD(config)# router ospf enable
```

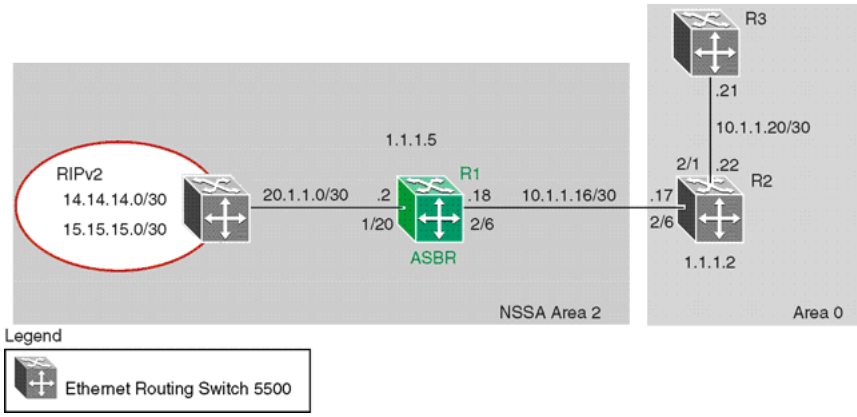
—End—

Not So Stubby Areas (NSSA) Similar to stub areas, the not so stubby area (NSSA) can also prevent the flooding of AS-External Link State advertisements into the NSSA by replacing them with a default route. However, NSSA can also import small stub (non-OSPF) routing domains into OSPF. This allows the NSSA to import external routes, such as RIP routes, and then advertise these routes throughout the network.

External routing information is imported into NSSA by using type 7 LSAs. These LSAs are translated at the NSSA boundary into LSA type 5. The N/P bit in the type 7 LSA Options field indicates whether the type 7 LSA must be translated. Only those LSAs with the N/P-bit set are translated.

The NSSA configuration example illustrated below demonstrates a Nortel Ethernet Routing Switch 5500 Series configured as a NSSA ASBR router.

NSSA configuration example



To configure the example illustrated above, follow this procedure:

Step	Action
1	Configure router R1.

a. Configure the RIP interface on R1.

Configure port 1/20 as a brouter port in VLAN 100 and enable RIP on this interface.

```
5530-24TFD(config)# interface fast 1/20
5530-24TFD(config-if)# brouter port 1/20 vlan 100
subnet 20.1.1.2/30
5530-24TFD(config)# router rip
5530-24TFD(config-router)# network 20.1.1.2
```

b. Enable RIP globally and configure the RIP version 2 interface.

```
5530-24TFD(config)# router rip enable
```

```
5530-24TFD(config)# interface vlan 100
5530-24TFD(config-if)# ip rip receive version rip2
send version rip2
```

c. Configure the OSPF interface on R1.

   Configure port 2/6 as a brouter port in VLAN 200.

```
5530-24TFD(config)# interface fast 2/6
5530-24TFD(config-if)# brouter port 2/6 vlan 200
subnet 10.1.1.18/30
```

d. Enable OSPF on R1.

   Configure R1 as an ASBR, assign OSPF Router-ID 1.1.1.5, create OSPF NSSA area 2, add the OSPF interface 10.1.1.18 to area 2, and enable OSPF on the interface.

```
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# as-boundary-router enable
5530-24TFD(config-router)# router-id 1.1.1.5
5530-24TFD(config-router)# area 0.0.0.2 import nssa
5530-24TFD(config-router)# network 10.1.1.18 area
0.0.0.2
5530-24TFD(config)# router ospf enable
```

e. Configure a route policy to distribute Direct and OSPF to RIP.

   Create a route policy named **Rip_Dist** that distributes directly connected and OSPF routes into RIP.

```
5530-24TFD(config)# route-map Rip_Dist permit 1
enable match protocol direct,ospf set metric-type
type1
```

f. Apply the **Rip_Dist** route policy to RIP Out Policy.

```
5530-24TFD(config)# interface vlan 100
5530-24TFD(config-if)# ip rip out-policy Rip_Dist
```

g. Configure OSPF route distribution to distribute RIP routes as AS-external LSA type 1.

```
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# redistribute rip enable
metric-type type1
5530-24TFD(config)# ip ospf apply redistribute rip
```

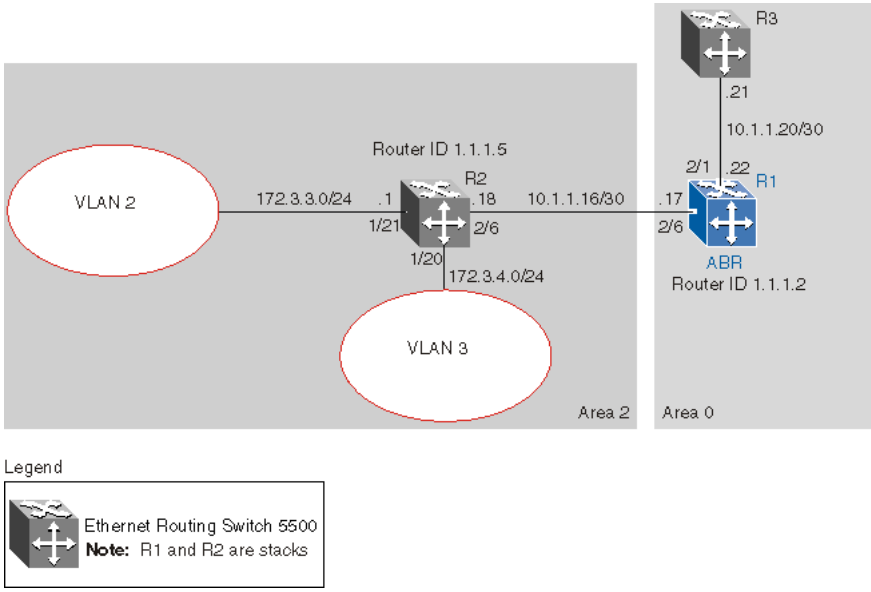
—End—

Configuring Area Border Routers (ABR)

Configuration of an OSPF ABR is an automatic process on the Nortel Ethernet Routing Switch 5500 Series; no user intervention is required. The Nortel Ethernet Routing Switch 5500 Series automatically becomes an OSPF ABR when it has operational OSPF interfaces belonging to more than one area.

In the configuration example below, the Nortel Ethernet Routing Switch 5500 Series R1 is automatically configured as an OSPF ABR after it is configured with an OSPF interface for area 0.0.0.0 and 0.0.0.2.

ABR configuration example



To recreate the illustrated ABR configuration, use the following procedure:

Step	Action

1	Configure an OSPF interface on port 2/6.
	Configure port 2/6 as a brouter port in VLAN 100.
	`5530-24TFD(config)# interface fast 2/6`
	`5530-24TFD(config-if)# brouter port 2/6 vlan 100 subnet 10.1.1.17/30`

2	Configure an OSPF interface on port 2/1.
	Configure port 2/1 as a brouter port in VLAN 200 and enable OSPF on this interface.
	`5530-24TFD(config)# interface fast 2/1`
	`5530-24TFD(config-if)# brouter port 2/1 vlan 200 subnet 10.1.1.22/30`
	`5530-24TFD(config-if)# ip ospf enable`

3 Enable OSPF.

Configure R1 as an ABR. Note that, by default, OSPF interface 10.1.1.22 is placed into OSPF area 0.0.0.0. Because one additional area of 0.0.0.2 is created and OSPF interface 10.1.1.17 is added to area 0.0.0.2, R1 automatically becomes an ABR.

```
5530-24TFD(config-router)#  router-id 1.1.1.2
5530-24TFD(config-router)# area 0.0.0.2
5530-24TFD(config-router)# network 10.1.1.17
area 0.0.0.2
5530-24TFD(config)# router ospf enable
```

4 Configure area range.

Configure R1 to enclose the two networks (172.3.3.0 and 172.3.4.0) into an address range entry 172.3.0.0 in area 0.0.0.2. R1 will generate a single summary advertisement into the backbone for 172.3.0.0 with metric 100.

```
5530-24TFD(config-router)# area 0.0.0.2 range
172.3.0.0/16 summary-link advertise-mode summarize
advertise-metric 100
```

—End—

To display the created areas, use the **show ip ospf area** command. Usage of this command on the example configuration would yield the following output:

```
Area ID:  0.0.0.0
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  2
Reachable Area Border Routers:  0
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  0
Link-State Advertisements Checksum:  0(0x0)
Area ID:  0.0.0.2
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  2
Reachable Area Border Routers:  1
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  0
Link-State Advertisements Checksum:  0(0x0)
```

To display area ranges, use the **show ip ospf area-range** command. Usage of this command on the example configuration would yield the following output:

```
Area ID      Range Subnet/Mask  Range Type    Advertise Mode Metric
-----------  -----------------  ------------  -------------- ------
0.0.0.2      172.3.0.0/16       Summary Link  Summarize      100
```

To display ABR status, use the **show ip ospf** command. Usage of this command on the example configuration would yield the following output:

```
Router ID:  1.1.1.2
Admin Status:  Enabled
Version Number:  2
Area Border Router Oper Status:  True
AS Boundary Router Config Status:  False
External Link-State Advertisements:  2
External Link-State Checksum:  45698(0xb282)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  5
New Link-State Advertisements Received:  34
OSPF Traps:  Disabled
Auto Virtual Link Creation:  Disabled
SPF Hold-Down Time:  10
RFC 1583 Compatibility:  Enabled
```

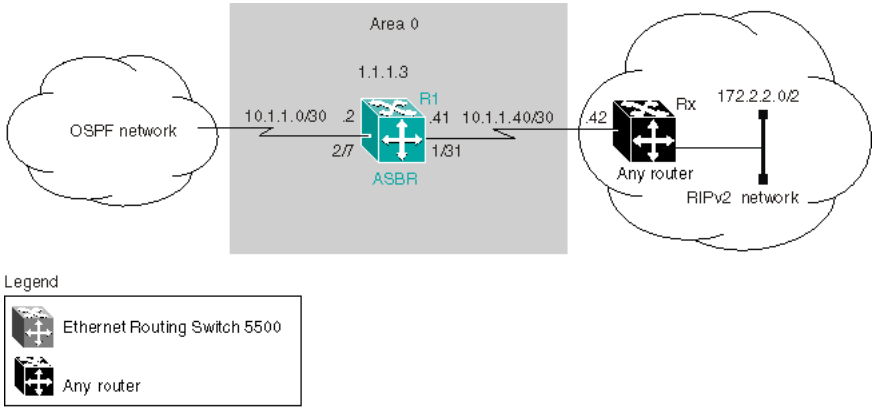
Configuring Autonomous System Border Routers (ASBR)

An ASBR is a router that has a connection to another Autonomous System to distribute any external routes that originated from a protocol into OSPF. A Nortel Ethernet Routing Switch 5500 Series configured as an ASBR can:

- Distribute all OSPF routes to RIP.
- Distribute RIP, direct, or static routes to OSPF.

Distributing OSPF routes to RIP and RIP to OSPF using AS-external LSA Type 1 metrics The configuration example illustrated below, displays a Nortel Ethernet Routing Switch 5500 Series configured as an ASBR between an OSPF and RIP version 2 network. In this example, the router distributes all OSPF routes to the RIP network and all RIP routes to the OSPF network.

ASBR distribution example



Use the following procedure to replicate the ASBR distribution example:

Step	Action

1	Configure RIP.
	
	Configure the RIP interface on R1 by configuring port 1/31 as a brouter port in VLAN 100 and enabling RIP on this interface.
	
	`5530-24TFD(config)# interface fast 1/31`
	`5530-24TFD(config-if)# brouter port 1/31 vlan 100 subnet 10.1.1.41/30`
	`5530-24TFD(config)# router rip`
	`5530-24TFD(config-router)# network 10.1.1.41`

2	Configure the RIP interface for RIP version 2 mode only.
	
	`5530-24TFD(config)# router rip enable`
	`5530-24TFD(config)# interface vlan 100`
	`5530-24TFD(config-if)# ip rip receive version rip2 send version rip2`

3	Configure the OSPF interface.
	
	Configure port 2/7 as a brouter port in VLAN 200 and enable OSPF on this interface.
	
	`5530-24TFD(config)# interface fast 2/7`
	`5530-24TFD(config-if)# brouter port 2/7 vlan 200 subnet 10.1.1.2/30`
	`5530-24TFD(config-if)# router ospf`
	`5530-24TFD(config-router)# network 10.1.1.2`

4	Make R1 the ASBR. Configure R1 as an ASBR and assign the OSPF Router-ID. `5530-24TFD(config)# router ospf`

```
5530-24TFD(config-router)# as-boundary-router enable
5530-24TFD(config-router)# router-id 1.1.1.3
5530-24TFD(config)# router ospf enable
```

5 Configure OSPF route distribution.

Configure OSPF route distribution to import RIP into OSPF. The Nortel Ethernet Routing Switch 5500 Series distributes the RIP routes as AS-external LSA (LSA type 5), using external metric type 1.

```
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# redistribute rip enable
metric 10 metric-type type1
5530-24TFD(config)# ip ospf apply redistribute rip
```

6 Configure a route policy.

A route policy is required for OSPF to RIP route redistribution. After the route policy is created, apply it to the RIP interface. The following command creates a route policy named **allow** which distributes both direct and OSPF interfaces.

```
5530-24TFD(config)# route-map allow permit 1 enable
match protocol direct,ospf
```

7 Apply the route policy to the RIP Out Policy.

The following commands apply the route policy created in step 6 to RIP interface 10.1.1.41.

```
5530-24TFD(config)# interface vlan 100
5530-24TFD(config-if)# ip rip out-policy allow
```

—End—

The configuration steps described in the above example distributes all OSPF routes to RIP. However, there are times when it can be more advantageous to distribute only a default route to RIP. The following configuration steps describe how to distribute only a default route to RIP instead of all OSPF routes to RIP.

To configure R1 to distribute a default route only to RIP, complete the following steps:

Step	Action

1 Configure an IP prefix list with a default route.

The following command creates an IP prefix list named **default** with an IP address of 0.0.0.0.

```
5530-24TFD(config)# ip prefix-list default 0.0.0.0/0
```

2 Configure a route policy.

Create a route policy named **Policy_Default** which distributes the IP prefix list created in step 1. Note that **ospf** is selected as the **match-protocol** value. This causes the default route to be advertised through RIP only if OSPF is operational.

```
5530-24TFD(config)# route-map Policy_Default permit 1
enable match protocol ospf set injectlist default
5530-24TFD(config)# route-map Policy_Default
1 set  metric-type type1
```

3 Apply the route policy to the RIP Out Policy.

Apply the route policy created in step 2 to RIP interface 10.1.1.41.

```
5530-24TFD(config)# interface vlan 100
5530-24TFD(config-if)# ip rip out-policy Policy_Default
```

—End—

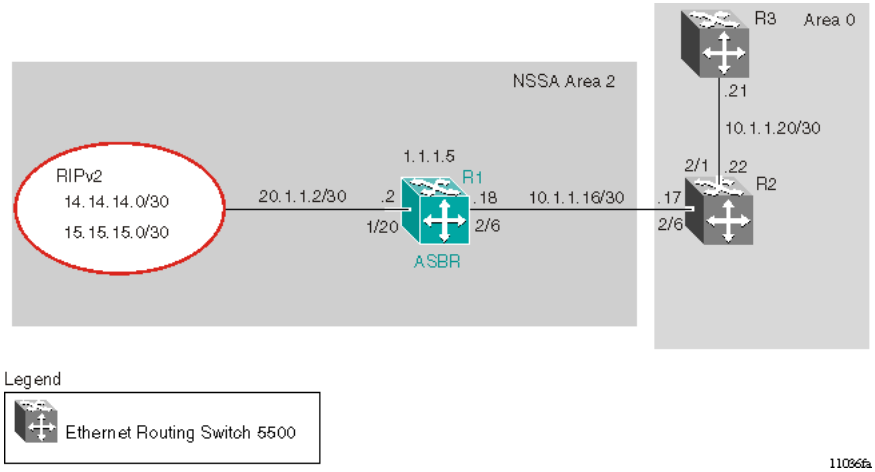
Controlling NSSA external route advertisements

In an OSPF NSSA, the NSSA N/p-bit (in the OSPF hello packets Options field) is used to tell the ABR which external routes can be advertised to other areas. When the NSSA N/p-bit is set true, the ABR exports the external route. This is the default setting for the Nortel Ethernet Routing Switch 5500 Series. When the NSSA N/p-bit is not set true, the ABR drops the external route. A route policy can be created on the Nortel Ethernet Routing Switch 5500 Series to manipulate the N/ p-bit value.

For example, the illustration below shows a RIP network located in NSSA 2. If advertising the 15.15.15.0/24 network to area 0 is the only desired action, perform the following tasks:

- Enable R1 as an OSPF ASBR.
- Create NSSA area 0.0.0.2.
- Create a route policy to advertise OSPF and direct interfaces to RIP.
- Create a route policy to only advertise RIP network 15.15.15.0/24 to area 0 by using the NSSA N/p-bit.

External route advertisement example



The following procedure outlines the commands used to replicate the above configuration example:

Step	Action

1	Configure the RIP interface.
	
	Configure port 1/20 as a brouter port in VLAN 200 and enables RIP on this interface.
	
	`5530-24TFD(config)# interface fast 1/20`
	`5530-24TFD(config-if)# brouter port 1/20 vlan 200 subnet 20.1.1.2/30`
	`5530-24TFD(config)# router rip`
	`5530-24TFD(config-router)# network 20.1.1.2`

2	Globally enable RIP and configure a RIP interface for RIP version 2.
	
	`5530-24TFD(config)# router rip enable`
	`5530-24TFD(config)# interface vlan 200`
	`5530-24TFD(config-if)# ip rip receive version rip2 send version rip2`

3	Configure the OSPF interface.
	
	Configure port 2/6 as a brouter port.
	
	`5530-24TFD(config)# interface fast 2/6`
	`5530-24TFD(config-if)# brouter port 2/6 vlan 100 subnet 10.1.1.18/30`

4	Enable OSPF.

Configure R1 as an ASBR, assign the OSPF Router-ID 1.1.1.5, create OSPF NSSA area 2, add the OSPF interface 10.1.1.18 to area 2, and enable OSPF on the interface. Enable ASBR and OSPF globally.

```
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# router-id 1.1.1.5
5530-24TFD(config-router)# as-boundary-router enable
5530-24TFD(config-router)# area 0.0.0.2 import nssa
5530-24TFD(config-router)# network 10.1.1.18 area
0.0.0.2
5530-24TFD(config)# router ospf enable
```

5 Create a route policy named **Rip_Dist** that distributes directly connected and OSPF routes into RIP.

```
5530-24TFD(config)# route-map Rip_Dist permit 1 enable
match protocol direct,ospf set metric-type type1
```

6 Apply route policy to RIP Out Policy.

```
5530-24TFD(config)# interface vlan 200
5530-24TFD(config-if)# ip rip out-policy Rip_Dist
```

7 Add two prefix lists (**15net** and **14net**) that are associated with the network addresses from the RIP version 2 network.

```
5530-24TFD(config)# ip prefix-list 15net 15.15.15.0/24
5530-24TFD(config)# ip prefix-list 14net 14.14.14.0/24
```

8 Create a route policy named **P_bit** that sets the NSSA N/P-bit only for the prefix list named **15net**.

```
5530-24TFD(config)# route-map P_bit permit 1 enable
match network 15net set nssa-pbit enable
5530-24TFD(config)# route-map P_bit permit 2 enable
match network 14net
5530-24TFD(config)# no route-map P_bit 2 set nssa-pbit
enable
```

9 Configure OSPF route distribution to distribute RIP routes as AS-external LSA Type 1.

```
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# redistribute rip enable
metric-type type1 route-policy P_bit
5530-24TFD(config)# ip ospf apply redistribute rip
```

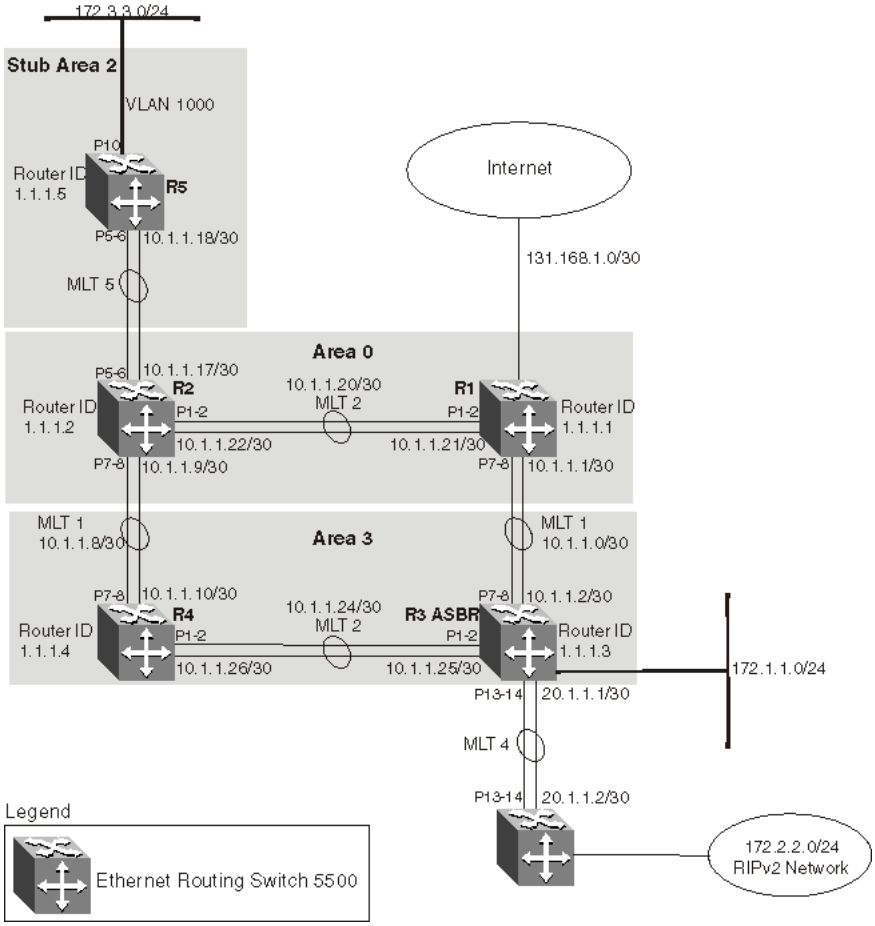
—End—

Configuring a multi-area complex

The multi-area complex configuration example described in this section uses five Nortel Ethernet Routing Switch 5500 Series devices (R1 to R5) in a multi-area configuration.

Many of the concepts and topology descriptions that are used in this example configuration are described in the previous sections of this chapter. The concepts shown in those examples are combined in this example configuration to show a real world topology example with command descriptions.

Multi-area complex example



For this configuration example, the Nortel Ethernet Routing Switch 5500 Series devices R1 through R5 are configured as follows:

- R1 is an OSPF ABR that is associated with OSPF Area 0 and 3.
- R2 is an OSPF Stub ABR for OSPF Area 2 and ABR to OSPF Area 3.
- R3 is an OSPF ASBR and is configured to distribute OSPF to RIP and RIP to OSPF.

- R4 is an OSPF internal router in Area 3.
- R5 is an internal OSPF stub router in Area 2.
- All interfaces used for this configuration are ethernet, therefore the OSPF interfaces are broadcast.
- The interface priority value on R5 is set to 0, therefore R5 cannot become a designated router (DR).
- Configure the OSPF Router Priority so that R1 becomes the DR (priority of 100) and R2 becomes backup designated router (BDR) with a priority value of 50.

Stub and NSSA areas are used to reduce the LSDB size by excluding external LSAs. The stub ABR advertises a default route into the stub area for all external routes.

The following list outlines the commands used to create the illustrated configuration. A similar listing could be provided by using the **`show running-config`** command.

1. R1 configuration commands

```
! *** STP (Phase 1) *** !
spanning-tree stp 2 create
spanning-tree stp 3 create
spanning-tree cost-calc-mode dot1d
spanning-tree port-mode normal
spanning-tree stp 1 priority 8000
spanning-tree stp 1 hello-time 2
spanning-tree stp 1 max-age 20
spanning-tree stp 1 forward-time 15
spanning-tree stp 1 tagged-bpdu disable
tagged-bpdu-vid 4001
spanning-tree stp 1 multicast-address 01:80:c2:00:00:00
spanning-tree stp 2 priority 8000
spanning-tree stp 2 hello-time 2
spanning-tree stp 2 max-age 20
spanning-tree stp 2 forward-time 15
spanning-tree stp 2 tagged-bpdu enable
tagged-bpdu-vid 4002
spanning-tree stp 2 multicast-address 01:80:c2:00:00:00
spanning-tree stp 3 priority 8000
spanning-tree stp 3 hello-time 2
spanning-tree stp 3 max-age 20
spanning-tree stp 3 forward-time 15
spanning-tree stp 3 tagged-bpdu enable
tagged-bpdu-vid 4003
spanning-tree stp 3 multicast-address 01:80:c2:00:00:00
! *** VLAN *** !
vlan configcontrol autopvid
auto-pvid
```

```
vlan name 1 "VLAN #1"
vlan create 102 name "VLAN #102" type port
vlan create 103 name "VLAN #103" type port
vlan ports 1-24 tagging unTagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan ports 25-26 tagging tagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan members 1 24-26
vlan members 102 1-2
vlan members 103 7-8
vlan ports 1-2 pvid 102
vlan ports 3-6 pvid 1
vlan ports 7-8 pvid 103
vlan ports 9-26 pvid 1
vlan igmp unknown-mcast-no-flood disable
vlan igmp 1 snooping disable
vlan igmp 1 proxy disable robust-value 2
query-interval 125
vlan igmp 102 snooping disable
vlan igmp 102 proxy disable robust-value 2
query-interval 125
vlan igmp 103 snooping disable
vlan igmp 103 proxy disable robust-value 2
query-interval 125
vlan mgmt 1
! *** MLT (Phase 1) *** !
no mlt
mlt 1 name "Trunk #1" enable member 7-8 learning normal
mlt 1 learning normal
mlt 1 bpdu all-ports
mlt 1 loadbalance basic
mlt 2 name "Trunk #2" enable member 1-2 learning normal
mlt 2 learning normal
mlt 2 bpdu all-ports
mlt 2 loadbalance basic
! *** STP (Phase 2) *** !
spanning-tree stp 1 add-vlan 1
spanning-tree stp 2 add-vlan 102
spanning-tree stp 3 add-vlan 103
spanning-tree stp 2 enable
spanning-tree stp 3 enable
interface FastEthernet ALL
spanning-tree port 24-26 learning normal
spanning-tree port 1-2 stp 2 learning normal
spanning-tree port 7-8 stp 3 learning normal
spanning-tree port 24-26 cost 1 priority 80
spanning-tree port 1-2 stp 2 cost 1 priority 80
spanning-tree port 7-8 stp 3 cost 1 priority 80
spanning-tree bpdu-filtering port 1-26 timeout 120
no spanning-tree bpdu-filtering port 1-26
```

```
enable
exit
! *** MLT (Phase 2) *** !
mlt spanning-tree 1 stp 3 learning normal
mlt spanning-tree 2 stp 2 learning normal
! *** L3 *** !
no ip directed-broadcast enable
ip routing
interface vlan 102
ip address 10.1.1.21 255.255.255.252 2
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 103
ip address 10.1.1.1 255.255.255.252 3
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
ip arp timeout 360
ip dhcp-relay
ip blocking-mode none
! *** OSPF *** !
router ospf enable
router ospf
router-id 1.1.1.1
no as-boundary-router enable
no trap enable
timers basic holddown 10
rfc1583-compatibility enable
default-cost ethernet 100
default-cost fast-ethernet 10
default-cost gig-ethernet 1
default-cost ten-gig-ethernet 1
area 0.0.0.3 import external
area 0.0.0.3 import-summaries enable
exit
enable
configure terminal
interface vlan 103
ip ospf area 0.0.0.3
ip ospf network broadcast
ip ospf priority 100
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf transmit-delay 1
ip ospf retransmit-interval 5
ip ospf hello-interval 10
```

```
ip ospf dead-interval 40
ip ospf enable
exit
interface vlan 102
ip ospf area 0.0.0.0
ip ospf network broadcast
ip ospf priority 100
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf enable
exit
```

2. R2 configuration commands

```
! ! *** STP (Phase 1) *** !
spanning-tree stp 2 create
spanning-tree cost-calc-mode dot1d
spanning-tree port-mode normal
spanning-tree stp 1 priority 8000
spanning-tree stp 1 hello-time 2
spanning-tree stp 1 max-age 20
spanning-tree stp 1 forward-time 15
spanning-tree stp 1 tagged-bpdu disable
tagged-bpdu-vid 4001
spanning-tree stp 1 multicast-address 01:80:c2:00:00:00
spanning-tree stp 2 priority 8000
spanning-tree stp 2 hello-time 2
spanning-tree stp 2 max-age 20
spanning-tree stp 2 forward-time 15
spanning-tree stp 2 tagged-bpdu enable
tagged-bpdu-vid 4002
spanning-tree stp 2 multicast-address 01:80:c2:00:00:00
! *** VLAN *** !
vlan configcontrol autopvid
auto-pvid
vlan name 1 "VLAN #1"
vlan create 100 name "VLAN #100" type port
vlan create 101 name "VLAN #101" type port
vlan create 102 name "VLAN #102" type port
vlan ports 1-2 tagging tagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan ports 3-6 tagging unTagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan ports 7-8 tagging tagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan ports 9-26 tagging unTagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan members 1 1-26
vlan members 100 5-6
vlan members 101 7-8
```

```
vlan members 102 1-2
vlan ports 1-2 pvid 102
vlan ports 3-4 pvid 1
vlan ports 5-6 pvid 100
vlan ports 7-8 pvid 101
vlan ports 9-26 pvid 1
vlan igmp unknown-mcast-no-flood disable
vlan igmp 1 snooping disable
vlan igmp 1 proxy disable robust-value 2
query-interval 125
vlan igmp 100 snooping disable
vlan igmp 100 proxy disable robust-value 2
query-interval 125
vlan igmp 101 snooping disable
vlan igmp 101 proxy disable robust-value 2
query-interval 125
vlan igmp 102 snooping disable
vlan igmp 102 proxy disable robust-value 2
query-interval 125
vlan mgmt 1
! *** MLT (Phase 1) *** !
no mlt
mlt 1 name "Trunk #1" enable member 7-8 learning normal
mlt 1 learning normal
mlt 1 bpdu all-ports
mlt 1 loadbalance basic
mlt 2 name "Trunk #2" enable member 1-2 learning normal
mlt 2 learning normal
mlt 2 bpdu all-ports
mlt 2 loadbalance basic
mlt 5 name "Trunk #5" enable member 5-6 learning normal
mlt 5 learning normal
mlt 5 bpdu all-ports
mlt 5 loadbalance basic
! *** STP (Phase 2) *** !
spanning-tree stp 1 add-vlan 1
spanning-tree stp 1 add-vlan 100
spanning-tree stp 2 add-vlan 101
spanning-tree stp 2 add-vlan 102
spanning-tree stp 2 enable
interface FastEthernet ALL
spanning-tree port 1-26 learning normal
spanning-tree port 1-2,7-8 stp 2 learning normal
spanning-tree port 1-26 cost 1 priority 80
spanning-tree port 1-2,7-8 stp 2 cost 1 priority 80
spanning-tree bpdu-filtering port 1-26 timeout 120
no spanning-tree bpdu-filtering port 1-26 enable
exit
! *** MLT (Phase 2) *** !
mlt spanning-tree 1 stp 1 learning normal
```

```
mlt spanning-tree 1 stp 2 learning normal
mlt spanning-tree 2 stp 1 learning normal
mlt spanning-tree 2 stp 2 learning normal
mlt spanning-tree 5 stp 1 learning normal
! *** L3 *** !
no ip directed-broadcast enable
ip routing
interface vlan 1
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 100
ip address 10.1.1.17 255.255.255.252 2
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 101
ip address 10.1.1.9 255.255.255.252 3
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 102
ip address 10.1.1.22 255.255.255.252 4
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
ip arp timeout 360
ip dhcp-relay
ip blocking-mode none
! *** ECMP *** !
maximum-path 1 rip
maximum-path 1 ospf
maximum-path 1
! *** OSPF *** !
router ospf enable
router ospf
router-id 1.1.1.2
no as-boundary-router enable
no trap enable
timers basic holddown 10
rfc1583-compatibility enable
default-cost ethernet 100
default-cost fast-ethernet 10
default-cost gig-ethernet 1
default-cost ten-gig-ethernet 1
area 0.0.0.2 import noexternal
```

```
default-cost 1
area 0.0.0.2 import-summaries enable
area 0.0.0.3 import external
area 0.0.0.3 import-summaries enable
exit
enable
configure terminal
interface vlan 101
ip ospf area 0.0.0.3
ip ospf network broadcast
ip ospf priority 50
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf transmit-delay 1
ip ospf retransmit-interval 5
ip ospf hello-interval 10
ip ospf dead-interval 40
ip ospf enable
exit
interface vlan 100
ip ospf area 0.0.0.2
ip ospf network broadcast
ip ospf priority 50
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf enable
exit
interface vlan 102
ip ospf area 0.0.0.0
ip ospf network broadcast
ip ospf priority 50
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf enable
exit
interface vlan 1
ip ospf area 0.0.0.0
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
no ip ospf enable
exit
```

3. R3 configuration commands

```
! *** STP (Phase 1) *** !
```

```
spanning-tree stp 3 create
spanning-tree cost-calc-mode dot1d
spanning-tree port-mode normal
spanning-tree stp 1 priority 8000
spanning-tree stp 1 hello-time 2
spanning-tree stp 1 max-age 20
spanning-tree stp 1 forward-time 15
spanning-tree stp 1 tagged-bpdu disable
tagged-bpdu-vid 4001
spanning-tree stp 1 multicast-address 01:80:c2:00:00:00
spanning-tree stp 3 priority 8000
spanning-tree stp 3 hello-time 2
spanning-tree stp 3 max-age 20
spanning-tree stp 3 forward-time 15
spanning-tree stp 3 tagged-bpdu enable
tagged-bpdu-vid 4003
spanning-tree stp 3 multicast-address 01:80:c2:00:00:00
! *** VLAN *** !
vlan configcontrol automatic
auto-pvid
vlan name 1 "VLAN #1"
vlan create 103 name "VLAN #103" type port
vlan create 104 name "VLAN #104" type port
vlan create 105 name "VLAN #105" type port
vlan create 1001 name "VLAN #1001" type port
vlan ports 1-2 tagging tagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan ports 3-6 tagging unTagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan ports 7-8 tagging tagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan ports 9-26 tagging unTagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan members 1 4-6,9,12,15-26
vlan members 103 7-8
vlan members 104 1-2
vlan members 105 13-14
vlan members 1001 10
vlan ports 1-2 pvid 104
vlan ports 3-6 pvid 1
vlan ports 7-8 pvid 103
vlan ports 9 pvid 1
vlan ports 10 pvid 1001
vlan ports 11-12 pvid 1
vlan ports 13-14 pvid 105
vlan ports 15-26 pvid 1
vlan igmp unknown-mcast-no-flood disable
vlan igmp 1 snooping disable
vlan igmp 1 proxy disable robust-value 2
query-interval 125
```

```
vlan igmp 103 snooping disable
vlan igmp 103 proxy disable robust-value 2
query-interval 125
vlan igmp 104 snooping disable
vlan igmp 104 proxy disable robust-value 2
query-interval 125
vlan igmp 105 snooping disable
vlan igmp 105 proxy disable robust-value 2
query-interval 125
vlan igmp 1001 snooping disable
vlan igmp 1001 proxy disable robust-value 2
query-interval 125
vlan mgmt 1
! *** MLT (Phase 1) *** !
no mlt
mlt 1 name "Trunk #1" enable member 7-8 learning normal
mlt 1 learning normal
mlt 1 bpdu all-ports
mlt 1 loadbalance basic
mlt 2 name "Trunk #2" enable member 1-2 learning normal
mlt 2 learning normal
mlt 2 bpdu all-ports
mlt 2 loadbalance basic
mlt 4 name "Trunk #4" enable member 13-14 learning normal
mlt 4 learning normal
mlt 4 bpdu all-ports
mlt 4 loadbalance basic
! *** STP (Phase 2) *** !
spanning-tree stp 1 add-vlan 1
spanning-tree stp 3 add-vlan 103
spanning-tree stp 3 add-vlan 104
spanning-tree stp 1 add-vlan 105
spanning-tree stp 1 add-vlan 1001
spanning-tree stp 3 enable
interface FastEthernet ALL
spanning-tree port 4-6,9,12-26 learning normal
spanning-tree port 1-2,7-8 stp 3 learning normal
spanning-tree port 4-6,9,12-26 cost 1 priority 80
spanning-tree port 1-2,7-8 stp 3 cost 1 priority 80
spanning-tree bpdu-filtering port 1-26 timeout 120
no spanning-tree bpdu-filtering port 1-26 enable
exit
interface FastEthernet ALL
spanning-tree port 10 learning disable
exit
interface FastEthernet ALL
exit
! *** MLT (Phase 2) *** !
mlt spanning-tree 1 stp 3 learning normal
mlt spanning-tree 2 stp 3 learning normal
```

```
mlt spanning-tree 4 stp 1 learning normal
! *** L3 *** !
no ip directed-broadcast enable
ip routing
interface vlan 1
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 103
ip address 10.1.1.2 255.255.255.252 3
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 104
ip address 10.1.1.25 255.255.255.252 4
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 105
ip address 20.1.1.1 255.255.255.0 5
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 1001
ip address 172.1.1.1 255.255.255.0 2
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
ip arp timeout 360
ip dhcp-relay
ip blocking-mode none
! *** Route Policies *** !
route-map Allow permit 1
route-map Allow 1 enable
route-map Allow 1 match protocol direct,ospf
no route-map Allow 1 match interface
route-map Allow 1 match metric 0
no route-map Allow 1 match network
no route-map Allow 1 match next-hop
route-map Allow 1 match route-type any
no route-map Allow 1 match route-source
no route-map Allow 1 set injectlist
route-map Allow 1 set mask 0.0.0.0
route-map Allow 1 set metric 5
route-map Allow 1 set nssa-pbit enable
```

```
route-map Allow 1 set ip-preference 0
! *** OSPF *** !
router ospf enable
router ospf
router-id 1.1.1.3
as-boundary-router enable
no trap enable
timers basic holddown 10
rfc1583-compatibility enable
default-cost ethernet 100
default-cost fast-ethernet 10
default-cost gig-ethernet 1
default-cost ten-gig-ethernet 1
area 0.0.0.0 import external
area 0.0.0.0 import-summaries enable
area 0.0.0.3 import external
area 0.0.0.3 import-summaries enable
redistribute direct metric 10 metric-type
type2 subnets allow
redistribute direct enable
redistribute rip metric 10 metric-type type2 subnets allow
redistribute rip enable
exit
enable
configure terminal
interface vlan 103
ip ospf area 0.0.0.3
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf transmit-delay 1
ip ospf retransmit-interval 5
ip ospf hello-interval 10
ip ospf dead-interval 40
ip ospf enable
exit
interface vlan 104
ip ospf area 0.0.0.3
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf enable
exit
interface vlan 105
ip ospf area 0.0.0.0
ip ospf network broadcast
```

```
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
no ip ospf enable
exit
interface vlan 1001
ip ospf area 0.0.0.3
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf enable
exit
interface vlan 1
ip ospf area 0.0.0.0
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
no ip ospf enable
exit
! *** RIP *** !
router rip
router rip enable
timers basic holddown 120
timers basic timeout 180 update 30
default-metric 8
no network 10.1.1.2
no network 10.1.1.25
network 20.1.1.1
no network 172.1.1.1
no network 203.203.100.52
exit
enable
configure terminal
interface vlan 103
no ip rip advertise-when-down enable
no ip rip auto-aggregation enable
no ip rip default-listen enable
no ip rip default-supply enable
ip rip cost 1
ip rip holddown 120
ip rip listen enable
no ip rip poison enable
no ip rip proxy-announce enable
ip rip receive version rip1OrRip2
ip rip send version rip1Comp
```

```
ip rip timeout 180
no ip rip triggered enable
ip rip supply enable
exit
interface vlan 104
no ip rip advertise-when-down enable
no ip rip auto-aggregation enable
no ip rip default-listen enable
no ip rip default-supply enable
ip rip cost 1
ip rip holddown 120
ip rip listen enable
no ip rip poison enable
no ip rip proxy-announce enable
ip rip receive version rip1OrRip2
ip rip send version rip1Comp
ip rip timeout 180
no ip rip triggered enable
ip rip supply enable
exit
interface vlan 105
no ip rip advertise-when-down enable
no ip rip auto-aggregation enable
no ip rip default-listen enable
no ip rip default-supply enable
ip rip cost 1
ip rip holddown 120
ip rip listen enable
ip rip out-policy Allow
no ip rip poison enable
no ip rip proxy-announce enable
ip rip receive version rip1OrRip2
ip rip send version rip1Comp
ip rip timeout 180
no ip rip triggered enable
ip rip supply enable
exit
interface vlan 1001
no ip rip advertise-when-down enable
no ip rip auto-aggregation enable
no ip rip default-listen enable
no ip rip default-supply enable
ip rip cost 1
ip rip holddown 120
ip rip listen enable
no ip rip poison enable
no ip rip proxy-announce enable
ip rip receive version rip1OrRip2
ip rip send version rip1Comp
ip rip timeout 180
```

```
no ip rip triggered enable
ip rip supply enable
exit
interface vlan 1
no ip rip advertise-when-down enable
no ip rip auto-aggregation enable
no ip rip default-listen enable
no ip rip default-supply enable
ip rip cost 1
ip rip holddown 120
ip rip listen enable
no ip rip poison enable
no ip rip proxy-announce enable
ip rip receive version rip1OrRip2
ip rip send version rip1Comp
ip rip timeout 180
no ip rip triggered enable
ip rip supply enable
exit
```

4. R4 configuration commands

```
! *** STP (Phase 1) *** !
spanning-tree stp 3 create
spanning-tree cost-calc-mode dot1d
spanning-tree port-mode normal
spanning-tree stp 1 priority 8000
spanning-tree stp 1 hello-time 2
spanning-tree stp 1 max-age 20
spanning-tree stp 1 forward-time 15
spanning-tree stp 1 tagged-bpdu disable
tagged-bpdu-vid 4001
spanning-tree stp 1 multicast-address 01:80:c2:00:00:00
spanning-tree stp 3 priority 8000
spanning-tree stp 3 hello-time 2
spanning-tree stp 3 max-age 20
spanning-tree stp 3 forward-time 15
spanning-tree stp 3 tagged-bpdu enable
tagged-bpdu-vid 4003
spanning-tree stp 3 multicast-address 01:80:c2:00:00:00
! *** VLAN *** !
vlan configcontrol automatic
auto-pvid
vlan name 1 "VLAN #1"
vlan create 101 name "VLAN #101" type port
vlan create 104 name "VLAN #104" type port
vlan ports 1-26 tagging unTagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan members 1 3-6,9-26
vlan members 101 7-8
vlan members 104 1-2
```

```
vlan ports 1-2 pvid 104
vlan ports 3-6 pvid 1
vlan ports 7-8 pvid 101
vlan ports 9-26 pvid 1
vlan igmp unknown-mcast-no-flood disable
vlan igmp 1 snooping disable
vlan igmp 1 proxy disable robust-value 2
query-interval 125
vlan igmp 101 snooping disable
vlan igmp 101 proxy disable robust-value 2
query-interval 125
vlan igmp 104 snooping disable
vlan igmp 104 proxy disable robust-value 2
query-interval 125
vlan mgmt 1
! *** MLT (Phase 1) *** !
no mlt
mlt 1 name "Trunk #1" enable member 7-8 learning normal
mlt 1 learning normal
mlt 1 bpdu all-ports
mlt 1 loadbalance basic
mlt 2 name "Trunk #2" enable member 1-2 learning normal
mlt 2 learning normal
mlt 2 bpdu all-ports
mlt 2 loadbalance basic
! *** STP (Phase 2) *** !
spanning-tree stp 1 add-vlan 1
spanning-tree stp 3 add-vlan 101
spanning-tree stp 3 add-vlan 104
spanning-tree stp 3 enable
interface FastEthernet ALL
spanning-tree port 3-6,9-26 learning normal
spanning-tree port 1-2,7-8 stp 3 learning normal
spanning-tree port 3-6,9-26 cost 1 priority 80
spanning-tree port 1-2,7-8 stp 3 cost 1 priority 80
spanning-tree bpdu-filtering port 1-26 timeout 120
no spanning-tree bpdu-filtering port 1-26 enable
exit
! *** MLT (Phase 2) *** !
mlt spanning-tree 1 stp 3 learning normal
mlt spanning-tree 2 stp 3 learning normal
! *** L3 *** !
no ip directed-broadcast enable
ip routing interface vlan 1
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 101
ip address 10.1.1.10 255.255.255.252 2
```

```
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 104
ip address 10.1.1.26 255.255.255.252 3
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
ip arp timeout 360
ip dhcp-relay ip blocking-mode none
! *** OSPF *** !
router ospf enable
router ospf
router-id 1.1.1.4
no as-boundary-router enable
no trap enable
timers basic holddown 10
rfc1583-compatibility enable
default-cost ethernet 100
default-cost fast-ethernet 10
default-cost gig-ethernet 1
default-cost ten-gig-ethernet 1
area 0.0.0.0 import external
area 0.0.0.0 import-summaries enable
area 0.0.0.3 import external
area 0.0.0.3 import-summaries enable
exit
enable
configure terminal
interface vlan 101
ip ospf area 0.0.0.3
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf transmit-delay 1
ip ospf retransmit-interval 5
ip ospf hello-interval 10
ip ospf dead-interval 40
ip ospf enable
exit
interface vlan 104
ip ospf area 0.0.0.3
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
```

```
no ip ospf advertise-when-down enable
ip ospf enable
exit
interface vlan 1
ip ospf area 0.0.0.0
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
no ip ospf enable
exit
```

5. R5 configuration commands

```
! *** STP (Phase 1) *** !
spanning-tree cost-calc-mode dot1d
spanning-tree port-mode normal
spanning-tree stp 1 priority 8000
spanning-tree stp 1 hello-time 2
spanning-tree stp 1 max-age 20
spanning-tree stp 1 forward-time 15
spanning-tree stp 1 tagged-bpdu disable
tagged-bpdu-vid 4001
spanning-tree stp 1 multicast-address 01:80:c2:00:00:00
! *** VLAN *** !
vlan configcontrol autopvid
auto-pvid
vlan name 1 "VLAN #1"
vlan create 100 name "VLAN #100" type port
vlan create 1000 name "VLAN #1000" type port
vlan ports 1-26 tagging unTagAll filter-untagged-frame
disable filter-unregistered-frames enable priority 0
vlan members 1 24-26
vlan members 100 5-6
vlan members 1000 10
vlan ports 1-4 pvid 1
vlan ports 5-6 pvid 100
vlan ports 7-9 pvid 1
vlan ports 10 pvid 1000
vlan ports 11-26 pvid 1
vlan igmp unknown-mcast-no-flood disable
vlan igmp 1 snooping disable
vlan igmp 1 proxy disable robust-value 2
query-interval 125
vlan igmp 100 snooping disable
vlan igmp 100 proxy disable robust-value 2
query-interval 125
vlan igmp 1000 snooping disable
```

```
vlan igmp 1000 proxy disable robust-value 2
query-interval 125
vlan mgmt 1
! *** MLT (Phase 1) *** !
mlt 5 name "Trunk #5" enable member 5-6 learning normal
mlt 5 learning normal
mlt 5 bpdu all-ports
mlt 5 loadbalance basic
! *** STP (Phase 2) *** !
spanning-tree stp 1 add-vlan 1
spanning-tree stp 1 add-vlan 100
spanning-tree stp 1 add-vlan 1000
interface FastEthernet ALL
spanning-tree port 5-6,24-26 learning normal
spanning-tree port 5-6,24-26 cost 1 priority 80
spanning-tree bpdu-filtering port 1-26 timeout 120
no spanning-tree bpdu-filtering port 1-26 enable
exit
interface FastEthernet ALL
spanning-tree port 10 learning disable
exit
! *** MLT (Phase 2) *** !
mlt spanning-tree 5 stp 1 learning normal
! *** L3 *** !
no ip directed-broadcast enable
ip routing interface vlan 1
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 100
ip address 10.1.1.18 255.255.255.252 2
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 1000
ip address 172.3.3.1 255.255.255.252 3
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
ip arp timeout 360
ip dhcp-relay
ip blocking-mode none
! *** OSPF *** !
router ospf enable
router ospf
router-id 1.1.1.5
no as-boundary-router enable
```

```
no trap enable
timers basic holddown 10
rfc1583-compatibility enable
default-cost ethernet 100
default-cost fast-ethernet 10
default-cost gig-ethernet 1
default-cost ten-gig-ethernet 1
area 0.0.0.0 import external
area 0.0.0.0 import-summaries enable
area 0.0.0.2 import noexternal
default-cost 1
area 0.0.0.2 import-summaries enable
exit
enable
configure terminal
interface vlan 100
ip ospf area 0.0.0.2
ip ospf network broadcast
ip ospf priority 0
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf transmit-delay 1
ip ospf retransmit-interval 5
ip ospf hello-interval 10
ip ospf dead-interval 40
ip ospf enable
exit
interface vlan 1000
ip ospf area 0.0.0.2
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
ip ospf enable
exit
interface vlan 1
ip ospf area 0.0.0.0
ip ospf network broadcast
ip ospf priority 1
ip ospf authentication-type none
ip ospf mtu-ignore enable
no ip ospf advertise-when-down enable
no ip ospf enable
exit
```

The following commands illustrate the status of the routers in the configuration example. Accompanying each command is the output matching to the configuration example.

Router R1 Status

show vlan

```
Id  Name      Type Protocol User PID Active IVL/SVL Mgmt
--- --------- ---- -------- -------- ------ ------- ----
1   VLAN #1   Port None     0x0000   Yes    IVL     Yes
Port Members: 1-2,5-7,9-14,16-17,19-26
2   VLAN #2   Port None     0x0000   Yes    IVL     No
Port Members: 3-4,8,18
5   VLAN #5   Port None     0x0000   Yes    IVL     No
Port Members: 15
```

Total VLANs:3

show vlan ip

```
================================================================================
Id  ifIndex Address        Mask           MacAddress      Offset Routing
================================================================================
Primary Interfaces
--------------------------------------------------------------------------------
1   10001   10.100.111.200 255.255.255.0  00:11:F9:35:84:40 1    Enabled
2   10002   3.3.3.1        255.255.255.0  00:11:F9:35:84:41 2    Enabled
5   10005   10.10.10.1     255.255.255.0  00:11:F9:35:84:44 5    Enabled
--------------------------------------------------------------------------------
Secondary Interfaces
--------------------------------------------------------------------------------
2   14096   4.4.4.1        255.255.255.0  00:11:F9:35:84:42 3    Enabled
2   18190   5.5.5.1        255.255.255.0  00:11:F9:35:84:43 4    Enabled
```

show ip ospf

```
Router ID:  1.1.1.1
Admin Status:  Enabled
Version Number:  2
Area Border Router Oper Status:  True
AS Boundary Router Config Status:  False
External Link-State Advertisements:  2
External Link-State Checksum:  49786(0xc27a)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  427
New Link-State Advertisements Received:  811
OSPF Traps:  Disabled
Auto Virtual Link Creation:  Disabled
SPF Hold-Down Time:  10
RFC 1583 Compatibility:  Enabled
```

show ip ospf area

```
Area ID:  0.0.0.0
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  35
Reachable Area Border Routers:  2
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  15
Link-State Advertisements Checksum:  551120(0x868d0)
Area ID:  0.0.0.3
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  37
Reachable Area Border Routers:  2
Reachable Autonomous System Border Routers:  1
Link-State Advertisements:  13
Link-State Advertisements Checksum:  454461(0x6ef3d)
```

show ip ospf interface

```
Interface:  10.1.1.1
Area ID:  0.0.0.3
Admin State:  Enabled
Type:  Broadcast
Priority:  100
Designated Router:  10.1.1.1
Backup Designated Router:  10.1.1.2
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  10.1.1.21
Area ID:  0.0.0.0
Admin State:  Enabled
Type:  Broadcast
Priority:  100
Designated Router:  10.1.1.21
Backup Designated Router:  10.1.1.22
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
```

show ip ospf neighbor

```
Interface Nbr Router ID Nbr IP Address Pri State RetransQLen Perm
--------- ------------- -------------- --- ----- ----------- ----
10.1.1.1  1.1.1.3       10.1.1.2       1   Full  0           Dyn
10.1.1.21 1.1.1.2       10.1.1.22      50  Full  0           Dyn
Total OSPF Neighbors:  2
```

show ip route

```
================================================================
                          Ip Route
================================================================
DST         MASK            NEXT      COST VLAN PORT PROT TYPE PRF
----------------------------------------------------------------
172.2.2.0   255.255.255.0   10.1.1.2  10   103  T#1  O    IB   120
172.1.1.0   255.255.255.0   10.1.1.2  20   103  T#1  O    IB    20
172.3.3.0   255.255.255.252 10.1.1.22 30   102  T#2  O    IB    25
20.1.1.0    255.255.255.0   10.1.1.2  10   103  T#1  O    IB   120
10.1.1.24   255.255.255.252 10.1.1.2  20   103  T#1  O    IB    20
10.1.1.20   255.255.255.252 10.1.1.21  1   102  ---- C    DB     0
10.1.1.16   255.255.255.252 10.1.1.22 20   102  T#2  O    IB    25
10.1.1.0    255.255.255.252 10.1.1.1   1   103  ---- C    DB     0
10.1.1.8    255.255.255.252 10.1.1.2  30   103  T#1  O    IB    20
Total Routes: 9
 ----------------------------------------------------------------
TYPE Legend: I=Indirect Route, D=Direct Route, A=Alternative Route,
B=Best Route, E=Ecmp Route, U=Unresolved Route, N=Not in HW
```

Router R2 Status

show vlan

```
Id  Name      Type Protocol User PID Active IVL/SVL Mgmt
--- --------- ---- -------- -------- ------ ------- ----
1   VLAN #1   Port None     0x0000   Yes    IVL     Yes
Port Members: 1-26
100 VLAN #100 Port None     0x0000   Yes    IVL     No
Port Members: 5-6
101 VLAN #101 Port None     0x0000   Yes    IVL     No
Port Members: 7-8
102 VLAN #102 Port None     0x0000   Yes    IVL     No
Port Members: 1-2
```

show vlan ip

```
Id ifIndex Address        Mask            MacAddress      Offset Routing
1  10001   203.203.100.53 255.255.255.0   00:15:9B:F3:70:40 1    Enabled
100 10100  10.1.1.17      255.255.255.252 00:15:9B:F3:70:41 2    Enabled
101 10101  10.1.1.9       255.255.255.252 00:15:9B:F3:70:42 3    Enabled
102 10102  10.1.1.22      255.255.255.252 00:15:9B:F3:70:43 4    Enabled
```

show ip ospf

```
Router ID:  1.1.1.2
Admin Status:  Enabled
Version Number:  2
Area Border Router Oper Status:  True
AS Boundary Router Config Status:  False
External Link-State Advertisements:  2
External Link-State Checksum:  49786(0xc27a)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  99
New Link-State Advertisements Received:  66
OSPF Traps:  Disabled
Auto Virtual Link Creation:  Disabled
SPF Hold-Down Time:  10
RFC 1583 Compatibility:  Enabled
```

show ip ospf area

```
Area ID:  0.0.0.0
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  8
Reachable Area Border Routers:  2
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  15
Link-State Advertisements Checksum:  551120(0x868d0)
Area ID:  0.0.0.2
Import Summaries:  Yes
Import Type:  No External
Intra-Area SPF Runs:  10
Reachable Area Border Routers:  1
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  9
Link-State Advertisements Checksum:  274851(0x431a3)
Stub Metric:  1
Stub Metric Type:  OSPF Metric
Area ID:  0.0.0.3
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  13
Reachable Area Border Routers:  2
Reachable Autonomous System Border Routers:  1
```

```
Link-State Advertisements:  13
Link-State Advertisements Checksum:  454461(0x6ef3d)
```

show ip ospf interface

```
Interface:  10.1.1.9
Area ID:  0.0.0.3
Admin State:  Enabled
Type:  Broadcast
Priority:  50
Designated Router:  10.1.1.9
Backup Designated Router:  10.1.1.10
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  10.1.1.17
Area ID:  0.0.0.2
Admin State:  Enabled
Type:  Broadcast
Priority:  50
Designated Router:  10.1.1.17
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  10.1.1.22
Area ID:  0.0.0.0
Admin State:  Enabled
Type:  Broadcast
Priority:  50
Designated Router:  10.1.1.21
Backup Designated Router:  10.1.1.22
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  203.203.100.53
Area ID:  0.0.0.0
Admin State:  Disabled
Type:  Broadcast
Priority:  1
Designated Router:  0.0.0.0
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
```

show ip ospf neighbor

```
Interface Nbr Router ID Nbr IP Address Pri State RetransQLen Perm
--------- ------------- -------------- --- ----- ----------- ----
10.1.1.9  1.1.1.4       10.1.1.10      1   Full  0           Dyn
10.1.1.17 1.1.1.5       10.1.1.18      0   Full  0           Dyn
10.1.1.22 1.1.1.1       10.1.1.21      100 Full  0           Dyn
Total OSPF Neighbors:  3
```

show ip route

```
================================================================================
                              Ip Route
================================================================================
DST            MASK             NEXT           COST VLAN PORT PROT TYPE PRF
--------------------------------------------------------------------------------
172.3.3.0      255.255.255.252 10.1.1.18        20 100  T#5  O    IB    20
172.2.2.0      255.255.255.0   10.1.1.10        10 101  T#1  O    IB   120
172.1.1.0      255.255.255.0   10.1.1.10        30 101  T#1  O    IB    20
203.203.100.0 255.255.255.0    203.203.100.53    1   1  ---- C    DB     0
20.1.1.0       255.255.255.0   10.1.1.10        10 101  T#1  O    IB   120
10.1.1.24      255.255.255.252 10.1.1.10        20 101  T#1  O    IB    20
10.1.1.20      255.255.255.252 10.1.1.22         1 102  ---- C    DB     0
10.1.1.16      255.255.255.252 10.1.1.17         1 100  ---- C    DB     0
10.1.1.8       255.255.255.252 10.1.1.9          1 101  ---- C    DB     0
10.1.1.0       255.255.255.252 10.1.1.10        30 101  T#1  O    IB    20
Total Routes: 10
--------------------------------------------------------------------------------
TYPE Legend: I=Indirect Route, D=Direct Route, A=Alternative Route,
B=Best Route,E=Ecmp Route, U=Unresolved Route, N=Not in HW
```

Router R3 Status

show vlan

```
Id   Name        Type Protocol User PID Active IVL/SVL Mgmt
---  ---------   ---- -------- -------- ------ ------- ----
1    VLAN #1     Port None     0x0000   Yes    IVL     Yes
Port Members: 4-6,9,12,15-26
103  VLAN #103   Port None     0x0000   Yes    IVL     No
Port Members: 7-8
104  VLAN #104   Port None     0x0000   Yes    IVL     No
Port Members: 1-2
105  VLAN #105   Port None     0x0000   Yes    IVL     No
Port Members: 13-14
1001 VLAN #1001  Port None     0x0000   Yes    IVL     No
  Port Members: 10
```

show vlan ip

```
Id  ifIndex Address        Mask             MacAddress    Offset Routing
1   10001   203.203.100.52 255.255.255.0    00:15:9B:F1:FC:40 1   Enabled
103 10103   10.1.1.2       255.255.255.252  00:15:9B:F1:FC:42 3   Enabled
104 10104   10.1.1.25      255.255.255.252  00:15:9B:F1:FC:43 4   Enabled
105 10105   20.1.1.1       255.255.255.0    00:15:9B:F1:FC:44 5   Enabled
1001 11001  172.1.1.1      255.255.255.0    00:15:9B:F1:FC:41 2   Enabled
```

show ip rip

```
Default Import Metric:  8
Domain:
HoldDown Time:  120
Queries:  0 Rip:  Enabled
Route Changes:  1
Timeout Interval:  180
Update Time:  30
```

show ip rip interface

```
IP Address      Enable Send           Receive      Advertise When Down
--------------- ------ -------------- ------------ -------------------
10.1.1.2        false  rip1Compatible rip1OrRip2   false
10.1.1.25       false  rip1Compatible rip1OrRip2   false
20.1.1.1        true   rip1Compatible rip1OrRip2   false
172.1.1.1       false  rip1Compatible rip1OrRip2   false
203.203.100.52  false  rip1Compatible rip1OrRip2   false
            RIP  Dflt   Dflt   Trigger AutoAgg
IP Address  Cost Supply Listen Update  Enable Supply Listen Poison Proxy
----------  ---- ------ ------ ------- ------ ------ ------ ------ -----
10.1.1.2       1 false  false  false   false   true   true   false false
10.1.1.25      1 false  false  false   false   true   true   false false
20.1.1.1       1 false  false  false   false   true   true   false false
172.1.1.1      1 false  false  false   false   true   true   false false
203.203.100.52 1 false  false  false   false   true   true   false false
IP Address      RIP In Policy
--------------  -------------
10.1.1.2
10.1.1.25
20.1.1.1
172.1.1.1
203.203.100.52
IP Address      RIP Out Policy
--------------  --------------
10.1.1.2
10.1.1.25
20.1.1.1        Allow
```

```
172.1.1.1
203.203.100.52
IP Address      Holddown Timeout
--------------- -------- -------
10.1.1.2        120      180
10.1.1.25       120      180
20.1.1.1        120      180
172.1.1.1       120      180
203.203.100.52  120      180
```

show route-map detail

```
================================================================
                      Route Policy
================================================================
  Name  Allow,   Id 1,   Seq 1
----------------------------------------------------------------
       Match:
                         enable : enable
                           mode : permit
                 match-protocol : direct,ospf
                match-interface :
                   match-metric : 0
                  match-network :
                  match-next-hop :
                match-route-type : any
                 match-route-src :
       Set:
                 set-injectlist :
                        set-mask : 0.0.0.0
                     set-metric : 5
                 set-metric-type : type2
                   set-nssa-pbit : enable
       set-metric-type-internal : 0
                  set-preference : 0
   ----------------------------------------------------------------
```

show ip ospf redistribute

```
Source Metric Metric Type Subnet   Enabled Route Policy
------ ------ ----------- -------- ------- ------------
Direct 10     Type 2      Allow    True
RIP    10     Type 2      Allow    True
```

show ip ospf

```
Router ID:  1.1.1.3
Admin Status:  Enabled
Version Number:  2
Area Border Router Oper Status:  False
AS Boundary Router Config Status:  True
External Link-State Advertisements:  2
External Link-State Checksum:  49786(0xc27a)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  9
New Link-State Advertisements Received:  39
OSPF Traps:  Disabled
Auto Virtual Link Creation:  Disabled
SPF Hold-Down Time:  10
RFC 1583 Compatibility:  Enabled
```

show ip ospf area

```
Area ID:  0.0.0.0
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  1
Reachable Area Border Routers:  0
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  0
Link-State Advertisements Checksum:  0(0x0)
Area ID:  0.0.0.3
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  4
Reachable Area Border Routers:  2
Reachable Autonomous System Border Routers:  1
Link-State Advertisements:  13
Link-State Advertisements Checksum:  448840(0x6d948)
```

show ip ospf

```
Interface:  10.1.1.2
Area ID:  0.0.0.3
Admin State:  Enabled
Type:  Broadcast
Priority:  1
Designated Router:  10.1.1.1
Backup Designated Router:  10.1.1.2
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  10.1.1.25
Area ID:  0.0.0.3
Admin State:  Enabled
Type:  Broadcast
```

```
Priority:  1
Designated Router:  10.1.1.26
Backup Designated Router:  10.1.1.25
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  20.1.1.1
Area ID:  0.0.0.0
Admin State:  Disabled
Type:  Broadcast
Priority:  1
Designated Router:  0.0.0.0
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  172.1.1.1
Area ID:  0.0.0.3
Admin State:  Enabled
Type:  Broadcast
Priority:  1
Designated Router:  172.1.1.1
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  203.203.100.52
Area ID:  0.0.0.0
Admin State:  Disabled
Type:  Broadcast
Priority:  1
Designated Router:  0.0.0.0
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
```

show ip ospf neighbor

```
Interface  Nbr Router ID Nbr IP Address Pri State RetransQLen Perm
---------  ------------- -------------- --- ----- ----------- ----
10.1.1.2   1.1.1.1       10.1.1.1       100 Full  0           Dyn
10.1.1.25  1.1.1.4       10.1.1.26      1   Full  0           Dyn
Total OSPF Neighbors:  2
```

show ip route

```
=============================================================================
                            Ip Route
=============================================================================
DST            MASK             NEXT          COST VLAN PORT PROT TYPE PRF
-----------------------------------------------------------------------------
172.2.2.0      255.255.255.0    20.1.1.2      2    105  T#4  R    IB   100
172.3.3.0      255.255.255.252  10.1.1.1      40   103  T#1  O    IB    25
172.1.1.0      255.255.255.0    172.1.1.1     1    1001 ---- C    DB     0
20.1.1.0       255.255.255.0    20.1.1.1      1    105  ---- C    DB     0
10.1.1.16      255.255.255.252  10.1.1.1      30   103  T#1  O    IB    25
10.1.1.20      255.255.255.252  10.1.1.1      20   103  T#1  O    IB    25
10.1.1.24      255.255.255.252  10.1.1.25     1    104  ---- C    DB     0
10.1.1.8       255.255.255.252  10.1.1.26     20   104  T#2  O    IB    20
10.1.1.0       255.255.255.252  10.1.1.2      1    103  ---- C    DB     0
Total Routes: 9
-----------------------------------------------------------------------------
TYPE Legend: I=Indirect Route, D=Direct Route, A=Alternative Route,
B=Best Route,E=Ecmp Route, U=Unresolved Route, N=Not in HW
```

Router R4 Status

show vlan

```
Id   Name        Type Protocol User PID Active IVL/SVL Mgmt
---  ---------   ---- -------- -------- ------ ------- ----
1    VLAN #1     Port None     0x0000   Yes    IVL     Yes
Port Members: 3-6,9-26
101  VLAN #101   Port None     0x0000   Yes    IVL     No
Port Members: 7-8
104  VLAN #104   Port None     0x0000   Yes    IVL     No
Port Members: 1-2
```

show vlan ip

```
Id  ifIndex Address         Mask             MacAddress      Offset Routing
1   10001   203.203.100.54 255.255.255.0    00:15:9B:F2:2C:40 1    Enabled
101 10101   10.1.1.10      255.255.255.252 00:15:9B:F2:2C:41 2    Enabled
104 10104   10.1.1.26      255.255.255.252 00:15:9B:F2:2C:42 3    Enabled
```

show ip ospf

```
Router ID:  1.1.1.4
Admin Status:  Enabled
```

```
Version Number:  2
Area Border Router Oper Status:  False
AS Boundary Router Config Status:  False
External Link-State Advertisements:  2
External Link-State Checksum:  45698(0xb282)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  5
New Link-State Advertisements Received:  34
OSPF Traps:  Disabled
Auto Virtual Link Creation:  Disabled
SPF Hold-Down Time:  10
RFC 1583 Compatibility:  Enabled
```

show ip ospf area

```
Area ID:  0.0.0.0
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  1
Reachable Area Border Routers:  0
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  0
Link-State Advertisements Checksum:  0(0x0)
Area ID:  0.0.0.3
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  3
Reachable Area Border Routers:  2
Reachable Autonomous System Border Routers:  1
Link-State Advertisements:  13
Link-State Advertisements Checksum:  409758(0x6409e)
```

show ip ospf interface

```
Interface:  10.1.1.10
Area ID:  0.0.0.3
Admin State:  Enabled
Type:  Broadcast
Priority:  1
Designated Router:  10.1.1.9
Backup Designated Router:  10.1.1.10
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  10.1.1.26
Area ID:  0.0.0.3
Admin State:  Enabled
Type:  Broadcast
Priority:  1
```

```
Designated Router:  10.1.1.25
Backup Designated Router:  10.1.1.26
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  203.203.100.54
Area ID:  0.0.0.0
Admin State:  Disabled
Type:  Broadcast
Priority:  1
Designated Router:  0.0.0.0
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
```

show ip ospf neighbor

```
Interface Nbr Router ID Nbr IP Address  Pri State     RetransQLen Perm
--------- ------------- --------------- --- --------- ----------- ----
10.1.1.10 1.1.1.2       10.1.1.9        50  Full      0           Dyn
10.1.1.26 1.1.1.3       10.1.1.25       1   Full      0           Dyn
Total OSPF Neighbors:  2
```

show ip route

```
================================================================================
                              Ip Route
================================================================================
DST            MASK             NEXT          COST VLAN PORT PROT TYPE PRF
--------------------------------------------------------------------------------
172.2.2.0      255.255.255.0    10.1.1.25     10   104  T#2  O    IB   120
172.3.3.0      255.255.255.252 10.1.1.9       30   101  T#1  O    IB    25
172.1.1.0      255.255.255.0    10.1.1.25     20   104  T#2  O    IB    20
20.1.1.0       255.255.255.0    10.1.1.25     10   104  T#2  O    IB   120
10.1.1.16      255.255.255.252 10.1.1.9       20   101  T#1  O    IB    25
10.1.1.20      255.255.255.252 10.1.1.9       20   101  T#1  O    IB    25
10.1.1.24      255.255.255.252 10.1.1.26       1   104  ---- C    DB     0
10.1.1.8       255.255.255.252 10.1.1.10       1   101  ---- C    DB     0
10.1.1.0       255.255.255.252 10.1.1.25     20   104  T#2  O    IB    20
Total Routes: 9
--------------------------------------------------------------------------------
TYPE Legend: I=Indirect Route, D=Direct Route, A=Alternative Route,
B=Best Route,E=Ecmp Route, U=Unresolved Route, N=Not in HW
```

Router R5 Status

show vlan

```
Id   Name        Type Protocol User PID Active IVL/SVL Mgmt
---  ----------- ---- -------- -------- ------ ------- ----
1    VLAN #1     Port None     0x0000   Yes    IVL     Yes
Port Members: 24-26
100  VLAN #100   Port None     0x0000   Yes    IVL     No
Port Members: 5-6
1000 VLAN #1000 Port None     0x0000   Yes    IVL     No
  Port Members: 10
```

show vlan ip

```
Id  ifIndex Address         Mask            MacAddress     Offset Routing
1   10001   203.203.100.51 255.255.255.0   00:15:9B:F8:1C:40 1   Enabled
100 10100   10.1.1.18      255.255.255.252 00:15:9B:F8:1C:41 2   Enabled
1000 11000   172.3.3.1     255.255.255.252 00:15:9B:F8:1C:42 3   Enabled
```

show ip ospf

```
Router ID:  1.1.1.5
Admin Status:  Enabled
Version Number:  2
Area Border Router Oper Status:  False
AS Boundary Router Config Status:  False
External Link-State Advertisements:  0
External Link-State Checksum:  0(0x0)
Type-of-Service (TOS) Routing Supported:  False
Originated Link-State Advertisements:  48
New Link-State Advertisements Received:  387
OSPF Traps:  Disabled
Auto Virtual Link Creation:  Disabled
SPF Hold-Down Time:  10
RFC 1583 Compatibility:  Enabled
```

show ip ospf area

```
Area ID:  0.0.0.0
Import Summaries:  Yes
Import Type:  External
Intra-Area SPF Runs:  3
Reachable Area Border Routers:  0
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  0
Link-State Advertisements Checksum:  0(0x0)
Area ID:  0.0.0.2
Import Summaries:  Yes
```

```
Import Type:  No External
Intra-Area SPF Runs:  11
Reachable Area Border Routers:  1
Reachable Autonomous System Border Routers:  0
Link-State Advertisements:  9
Link-State Advertisements Checksum:  274851(0x431a3)
Stub Metric:  1
Stub Metric Type:  OSPF Metric
```

show ip ospf interface

```
Interface:  10.1.1.18
Area ID:  0.0.0.2
Admin State:  Enabled
Type:  Broadcast
Priority:  0
Designated Router:  10.1.1.17
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  172.3.3.1
Area ID:  0.0.0.2
Admin State:  Enabled
Type:  Broadcast
Priority:  1
Designated Router:  172.3.3.1
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
Interface:  203.203.100.51
Area ID:  0.0.0.0
Admin State:  Disabled
Type:  Broadcast
Priority:  1
Designated Router:  0.0.0.0
Backup Designated Router:  0.0.0.0
Authentication Type:  None
MTU Ignore:  Yes
Advertise When Down:  No
Metric Value:  10
```

show ip ospf

```
Interface Nbr Router ID   Nbr IP Address  Pri State     RetransQLen Perm
--------- --------------- --------------- --- --------- ----------- ----
10.1.1.18 1.1.1.2         10.1.1.17       50  Full      0           Dyn
Total OSPF Neighbors:  1
```

show ip route

```
================================================================================
                              Ip Route
================================================================================
DST            MASK             NEXT           COST VLAN PORT PROT TYPE PRF
--------------------------------------------------------------------------------
172.3.3.0      255.255.255.252 172.3.3.1       1    1000 ---- C    DB     0
172.1.1.0      255.255.255.0   10.1.1.17       40   100  T#5  O    IB     25
10.1.1.16      255.255.255.252 10.1.1.18       1    100  ---- C    DB     0
10.1.1.24      255.255.255.252 10.1.1.17       30   100  T#5  O    IB     25
10.1.1.20      255.255.255.252 10.1.1.17       20   100  T#5  O    IB     25
10.1.1.8       255.255.255.252 10.1.1.17       20   100  T#5  O    IB     25
10.1.1.0       255.255.255.252 10.1.1.17       40   100  T#5  O    IB     25
0.0.0.0        0.0.0.0         10.1.1.17       11   100  T#5  O    IB     25
Total Routes: 8
--------------------------------------------------------------------------------
TYPE Legend: I=Indirect Route, D=Direct Route, A=Alternative Route,
B=Best Route,E=Ecmp Route, U=Unresolved Route, N=Not in HW
```

Diagnosing neighbor state problems

At initial startup, routers transmit hello packets in an attempt to find other OSPF routers with which form adjacencies. After the hello packets are received, the routers perform an initialization process, which causes the routers to transition through various states before the adjacency is established. The following table lists the states a router can go through during the process of forming an adjacency.

OSPF neighbor states

Step	State	Description
1	Down	Indicates that a neighbor was configured manually, but the router did not received any information from the other router. This state can occur only on NBMA interfaces.
2	Attempt	On an NBMA interface, this state occurs when the router attempts to send unicast hellos to any configured interfaces. The Nortel Ethernet Routing Switch 5500 Series does not support NBMA type.

3	Init	The router received a general hello packet (without its Router ID) from another router.
4	2-Way	The router received a Hello directed to it from another router. (The hello contains its Router ID)
5	ExStart	Indicates the start of the Master/Slave election process.
6	Exchange	Indicates the link state database (LSDB) is exchanged
7	Loading	Indicates the processing state of the LSDB for input into the routing table. The router can request LSA for missing or corrupt routes.
8	Full	Indicates the normal full adjacency state.

OSPF neighbor state information Neighbor state information can be accessed by using the **`show ip ospf neighbor`** command.

```
5530-24TFD#show ip ospf neighbor
Interface Nbr Router ID Nbr IP Address Pri State RetransQLen Perm
--------- ------------- -------------- --- ----- ----------- ----
10.1.1.22 1.1.1.1       10.1.1.21      100 Full  0           Dyn
10.1.1.17 1.1.1.5       10.1.1.18      0   Full  0           Dyn
10.1.1.9  1.1.1.4       10.1.1.10      1   Full  0           Dyn
```

Problems with OSPF occur most often during the initial startup, when the router cannot form adjacencies with other routers and the state is stuck in the **Init** or **ExStart/Exchange** state.

Init State Problems A router can become stuck in an **Init** state and not form adjacencies. There are several possible causes for this problem:

- Authentication mismatch or configuration problem
- Area mismatch for Stub or NSSA
- Area ID mismatch
- Hello Interval or Dead Interval mismatch

To determine any mismatches in OSPF configuration, use the **`show ip ospf ifstats mismatch`** command.

ExStart/Exchange problems Even though routers can recognize each other and have moved beyond two way communications, routers can become stuck in the **ExStart/Exchange** state.

A mismatch in maximum transmission unit (MTU) sizes between the routers usually causes this type of problem. For example, one router could be set for a high MTU size and the other router a smaller value. Depending on the size of the link state database, the router with the smaller value may not be able to process the larger packets and thus be stuck in this state. To avoid this problem, ensure that the MTU size value for both routers match. This problem is usually encountered during interoperations in networks with other vendor devices.

> ***Note:*** The Nortel Ethernet Routing Switch 5500 Series automatically checks for OSPF MTU mismatches.

In the Nortel Ethernet Routing Switch 5500 Series, the supported MTU size for OSPF is 1500 bytes by default. Incoming OSPF database description (DBD) packets are dropped if their MTU size is greater than this value.

Virtual Router Redundancy Protocol (VRRP) configuration

This section describes how to create a basic VRRP configuration on a Nortel Ethernet Routing Switch 5500 Series.

VRRP uses an election process to select a master router that hosts use as the default gateway. If the master router (the default gateway) fails, the VRRP backup router automatically replaces the master router and becomes the new default gateway. In either case, the default gateway IP address and MAC address does not change, thereby providing transparent operation.

The Nortel Ethernet Routing Switch 5500 Series can be configured in a master-master configuration for load-balancing applications that use Split MultiLink Trunking (SMLT). This configuration allows both switches to respond to ARPs and forward traffic.

VRRP Priority settings can be configured to select the VRRP master router for a specified VLAN. The VRRP Priority setting is an integer value, in the range 1 and 255, where the highest value is used to elect the VRRP master router. If two or more switches have the same priority value, the switch with the highest numerical IP address value is selected and becomes the VRRP master. The host is unaware of the entire process.

When a host sends traffic to a different subnet, it sends an ARP request for the MAC address of the default gateway. In this case, the Nortel Ethernet Routing Switch 5500 Series VRRP master router replies with its virtual MAC address. The benefit of using a virtual MAC address is that, if the master router fails, the VRRP backup router uses the same virtual MAC address. The virtual MAC address on the Nortel Ethernet Routing Switch 5500 Series does not need to be configured. The virtual MAC address is automatically set as:

```
00-00-5E-00-01-<VRID>
```

Where the **VRID** is an integer value in the range 1 to 255 that represents the virtual router identification.

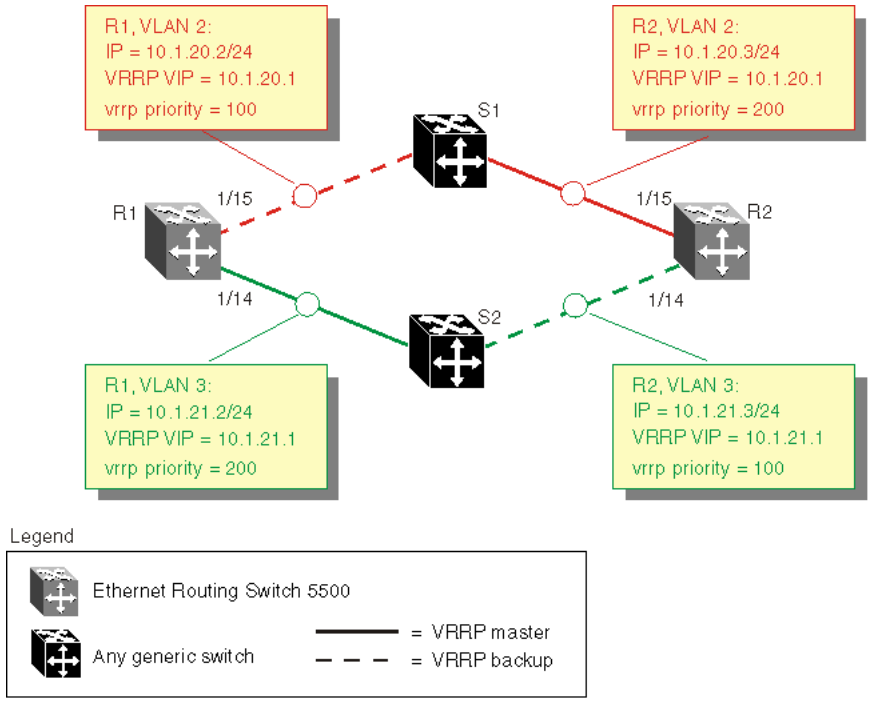
The virtual MAC address is assigned when VRRP is configured on a switch port or VLAN. The following example represents this process:

```
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan  2
5530-24TFD(config-if)# ip vrrp address 199 10.1.20.1
5530-24TFD(config-if)# ip vrrp 199 enable
```

Configuring normal VRRP operation

The following configuration example (illustrated below) shows how to provide VRRP service for two edge host locations.

VRRP example topology



In this example, the switches have the following duties:

- R1 is the VRRP master for S2
- R2 is the VRRP master for S1

In this example, VRRP is enabled with OSPF as the routing protocol on R1 and R2.

The VRRP priority setting is used to determine which router will become the VRRP master and which will become the VRRP backup. In instances where the priority setting is the same for two routers, the higher IP address becomes the tie breaker. Therefore, it is very important to set the correct VRRP priority. VRRP fast advertisement will also be enabled in this example to allow for fast failover detection.

The following procedure outlines the steps necessary to reproduce the example described above:

Step	Action

1 Configure VLAN 2 on router R1.

a. Create VLAN 2 on router R1.

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan create 2 type port
```

b. Configure the ports for VLAN 2 on R1.

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan members add 2 1/15
```

c. Configure an IP address for VLAN 2.

Add IP address 10.1.20.2 / 255.255.255.0 to VLAN 2.

```
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip address 10.1.20.2
255.255.255.0
```

d. Configure an OSPF interface for VLAN 2.

```
5530-24TFD# config terminal
5530-24TFD(config)# router ospf enable
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# network 10.1.20.2
```

e. Configure VRRP on VLAN 2.

The VRRP VIP address of 10.1.20.1 is added to VLAN 2 using a VRID of 1.

Note 1: The VRRP priority is not configured here; it is left at factory default of 100. Instead, the priority setting on router R2 will be set to a higher value when R2 is configured.

Note 2: Fast advertisement is disabled by default. Fast advertisement is proprietary to Nortel to support an advertisement interval from 200 to 1000 milliseconds (ms) with a default of 200. If fast VRRP advertisement is desired, enable fast advertisement.

```
5530-24TFD# config terminal
5530-24TFD(config)# router vrrp ena
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip vrrp address 1 10.1.20.1
5530-24TFD(config-if)# ip vrrp 1 enable
```

2 Configure VLAN 3 on router R1.

a. Configure VLAN 3 on router R1 using spanning tree group 1.

```
5530-24TFD# config terminal
5530-24TFD# vlan create 3 type port
```

b. Configure the ports for VLAN 3 on R1.

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan members add 3 1/14
```

c. Configure an IP address for VLAN 3.

Add IP address 10.1.21.2 / 255.255.255.0 to VLAN 3.

```
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 3
5530-24TFD(config)# ip address 10.1.21.2
255.255.255.0
```

d. Configure an OSPF interface for VLAN 3.

```
5530-24TFD# config terminal
5530-24TFD(config)# router ospf enable
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# network 10.1.21.2
```

e. Configure VRRP on VLAN 3.

The VRRP VIP address of 10.1.21.1 is added to VLAN 2 using a VRID of 2.

> ***Note:*** Fast advertisement is disabled by default. Fast advertisement is proprietary to Nortel to support an advertisement interval from 200 to 1000 milliseconds (ms) with a default of 200. If fast VRRP advertisement is desired, enable fast advertisement.

```
5530-24TFD# config terminal
5530-24TFD(config)# router vrrp ena
5530-24TFD(config)# interface vlan 3
5530-24TFD(config-if)# ip vrrp address 2 10.1.21.1
5530-24TFD(config-if)# ip vrrp 2 priority 200
5530-24TFD(config-if)# ip vrrp 2 enable
```

3 Configure VLAN 2 on router R2.

a. Create VLAN 2 on router R2.

```
5530-24TFD# config terminal
```

```
5530-24TFD(config)# vlan create 2 type port
```

b. Configure the ports for VLAN 2 on R2.

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan members add 2 1/15
```

c. Configure an IP address for VLAN 2.

Add IP address 10.1.20.3 / 255.255.255.0 to VLAN 2.

```
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip address 10.1.20.3
255.255.255.0
```

d. Configure an OSPF interface for VLAN 2.

```
5530-24TFD# config terminal
5530-24TFD(config)# router ospf enable
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# network 10.1.20.3
```

e. Configure VRRP on VLAN 2.

The VRRP VIP address of 10.1.21.1 is added to VLAN 2 using a VRID of 1.

Note 1: For this example the VRRP priority value is set to 200. This allows router R2 to be elected as the VRRP master router.

Note 2: Fast advertisement is disabled by default. Fast advertisement is proprietary to Nortel to support an advertisement interval from 200 to 1000 milliseconds (ms) with a default of 200. If fast VRRP advertisement is desired, enable fast advertisement.

```
5530-24TFD# config terminal
5530-24TFD(config)# router vrrp ena
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip vrrp address 1 10.1.20.1
5530-24TFD(config-if)# ip vrrp 1 enable
5530-24TFD(config-if)# ip vrrp 1 priority 200
```

4 Configure VLAN 3 on router R2.

a. Configure VLAN 3 on router R2.

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan create 3 type port
```

b. Configure the ports for VLAN 3 on R1.

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan members add 3 1/14
```

c. Configure an IP address for VLAN 3.

Add IP address 10.1.21.3 / 255.255.255.0 to VLAN 3.

```
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 3
5530-24TFD(config-if)# ip address 10.1.21.3
255.255.255.0
```

d. Configure an OSPF interface for VLAN 3.

```
5530-24TFD# config terminal
5530-24TFD(config)# router ospf enable
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# network 10.1.21.3
```

e. Configure VRRP on VLAN 3.

The VRRP VIP address of 10.1.21.1 is added to VLAN 2 using a VRID of 2.

Note: Fast advertisement is disabled by default. Fast advertisement is proprietary to Nortel to support an advertisement interval from 200 to 1000 milliseconds (ms) with a default of 200. If fast VRRP advertisement is desired, enable fast advertisement.

```
5530-24TFD# config terminal
5530-24TFD(config)# router vrrp ena
5530-24TFD(config)# interface vlan 3
5530-24TFD(config-if)# ip vrrp address 2 10.1.21.1
5530-24TFD(config-if)# ip vrrp 2 enable
```

—End—

After the VRRP configuration has been completed, use the **`show ip vrrp`** and **`show ip vrrp interface verbose`** commands to display VRRP configuration information and statistics.

Configuration command listing This following list is a complete sequence of the commands used in this configuration:

1. VLAN Configuration for Router R1

```
config t
vlan create 2 type port
vlan members remove 2 1/1-1/14,2/1-2/8,3/1-3/8
vlan members add 2 1/15 interface
vlan 2 ip address 10.1.20.2 255.255.255.0
router ospf enable
router ospf
network 10.1.20.2
```

```
router vrrp ena
interface vlan 2
ip vrrp address 1 10.1.20.1
ip vrrp 1 enable
vlan create 3 type port
interface vlan 3
ip address 10.1.21.2 255.255.255.0
router ospf enable
router ospf
network 10.1.21.2
router vrrp ena
interface vlan 3
ip vrrp address 2 10.1.21.1
ip vrrp 2 priority 200
ip vrrp 2 enable
```

2. VLAN Configuration for Router R2

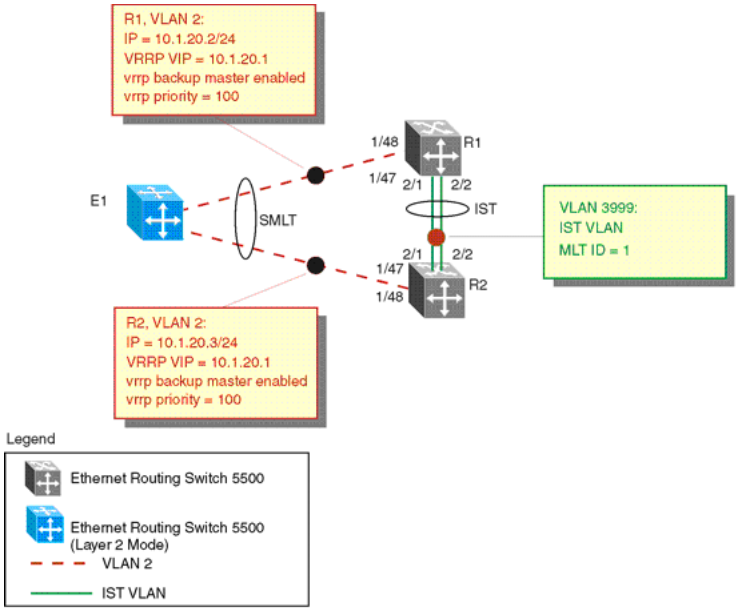
```
config t
vlan create 2 type port
vlan members remove 2 1/1-1/14,2/1-2/8,3/1-3/8
vlan members add  2 1/15 interface vlan 2
ip address 10.1.20.3 255.255.255.0
router ospf enable
router ospf
network 10.1.20.3
router vrrp ena
interface vlan 2
ip vrrp address 1 10.1.20.1
ip vrrp 1 priority 200
ip vrrp 1 enable
vlan create 3 type port
vlan members remove 3 1/1-1/14,1/15,2/1-2/8,3/1-3/8
vlan members add 3 1/14
interface vlan 3
ip address 10.1.21.3 255.255.255.0
router ospf enable
router ospf
network 10.1.21.3
router vrrp ena
interface vlan 3
ip vrrp address 2 10.1.21.1
ip vrrp 2 enable
```

Configuring VRRP with SMLT

This configuration example shows how you can provide high availability for a Layer 2 edge switch feeding into a Layer 3 core. As demonstrated below, both R1 and R2 switches are configured with a port-based VLAN (VLAN 2) with SMLT and VRRP set to enabled. This topology provides failover protection and load-balancing.

The Nortel Ethernet Routing Switch 5500 Series (E1), running in Layer 2 mode, is configured with one port-based VLAN and one MultiLink Trunking (MLT) group for the aggregate uplink ports. The Nortel Ethernet Routing Switch 5500 Series switches (R1 and R2) are configured with backup master enabled so that both switches can reply to ARP.

VRRP with SMLT configuration



The following procedure would be used to recreate the illustrated topology:

Step	Action

1 Configure the IST VLAN on R1

a. Configure IST VLAN 3999 on R1

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan create 3999 type port
5530-24TFD(config)# interface vlan 3999
5530-24TFD(config-if)# ip address 2.1.1.1
255.255.255.0
```

b. Configure IST MLT on R1

```
5530-24TFD# config terminal
5530-24TFD(config)# mlt 1 member 2/1-2/2
5530-24TFD(config)# vlan port 2/1-2/2 tagging enable
5530-24TFD(config)# mlt 1 enable
```

c. Configure the IST and add the IST to VLAN 3999

```
5530-24TFD# config terminal
5530-24TFD(config)# interface mlt 1
```

```
5530-24TFD(config-if)# ist enable peer-ip 2.1.1.2
vlan 3999
```

2 Configure VRRP and SMLT for access VLAN to E1

a. Configure VLAN 2 on R1

```
5530-24TFD# config terminal
5530-24TFD(config)#  vlan create 2 type port
```

b. Create IP address for VLAN 2

```
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip  address  10.1.20.2
255.255.255.0
```

c. Configure the access port for VLAN 2 on R1 and add VLAN 2 to the IST and SMLT groups

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan members add 2
1/48,1/47,2/1,2/2
```

Note: 2/1 and 2/2 are IST ports. 1/48,1/47 are SMLT ports.

d. Create SMLT on R1

```
5530-24TFD# config terminal
5530-24TFD(config)# mlt 2 member 1/47,1/48
5530-24TFD(config)# mlt 2 enable
5530-24TFD(config)# interface mlt 2
5530-24TFD(config-if)# smlt 1
```

e. Enable OSPF interface on VLAN 2 of R1

```
5530-24TFD# config terminal
5530-24TFD(config)# router ospf enable
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# network 10.1.20.2
```

f. Configure VRRP VIP address for VLAN2 of R1

```
5530-24TFD# config terminal
5530-24TFD(config)# router vrrp ena
5530-24TFD(config)# interface vlan 2
5530-24TFD(config)# ip vrrp address 1 10.1.20.1
5530-24TFD(config)# ip vrrp 1 enable
5530-24TFD(config)# ip vrrp 1 backup-master enable
```

Note: Fast advertisement is disabled by default. Fast advertisement is proprietary to Nortel to support an advertisement interval from 200 to 1000 milliseconds (ms) with a default of 200. If fast VRRP advertisement is desired, enable fast advertisement.

3 Configure the IST VLAN for router R2

a. Configure IST VLAN 3999 on R2

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan create 3999 type port
5530-24TFD(config)# interface vlan 3999
5530-24TFD(config-if)# ip address 2.1.1.2
255.255.255.0
```

b. Configure IST MLT on R2

```
5530-24TFD# config terminal
5530-24TFD(config)# mlt 1 member 2/1-2/2
5530-24TFD(config)# mlt 1 enable
5530-24TFD(config)# vlan port 2/1-2/2 tagging enable
```

c. Configure an IST peer for R2 and add the IST to VLAN 3999

```
5530-24TFD# config terminal
5530-24TFD(config)# interface mlt 1
5530-24TFD(config-if)# ist enable peer-ip 2.1.1.2
vlan 3999
```

4 Configure VRRP and SMLT for VLAN access to E1

a. Configure VLAN 2 on R2

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan create 2 type port
```

b. Create an IP address for VLAN 2

```
5530-24TFD# config terminal
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip address 10.1.20.3
255.255.255.0
```

c. Configure the access port for VLAN 2 on R2 and add VLAN 2 to the IST and SMLT groups

```
5530-24TFD# config terminal
5530-24TFD(config)# vlan members add 2 1/47, 1/48,
2/1.  2/2
```

Note: 1/47 and 1/48 are SMLT ports. 2/1 and 2/2 are IST ports.

d. Create SMLT on R2

```
5530-24TFD# config terminal
5530-24TFD(config)# mlt 2 member 1/47, 1/48
5530-24TFD(config)# mlt 2 enable
5530-24TFD(config)# interface mlt 2
5530-24TFD(config-if)# smlt 1
```

e. Enable OSPF interface for VLAN 2 on R2

```
5530-24TFD# config terminal
5530-24TFD(config)# router ospf enable
5530-24TFD(config)# router ospf
5530-24TFD(config-router)# network 10.1.20.3
```

f. Configure VRRP VIP address for VLAN 2 on R2

```
5530-24TFD# config terminal
5530-24TFD(config)# router vrrp ena
5530-24TFD(config)# interface vlan 2
5530-24TFD(config-if)# ip vrrp address 1 10.1.20.1
5530-24TFD(config-if)# ip vrrp 1 enable
5530-24TFD(config-if)# ip vrrp 1 backup-master
enable
```

Note: Fast Advertisement is disabled by default. Fast advertisement is proprietary to Nortel to support an advertisement interval from 200 to 1000 milliseconds (ms) with a default of 200. If fast VRRP advertisement is desired, enable fast advertisement.

—End—

Configuration command listing This following list is a complete sequence of the commands used in this configuration:

1. Configuration for R1

```
#MLT CONFIGURATION #
config t
mlt 1 member 2/1-2/2
mlt 1 ena
vlan port 2/2-2/2 tagging enable
interface mlt 1
ist enable peer-ip 2.1.1.2 vlan 3999
mlt 2 member 1/48,1/47
mlt 2 enable
interface mlt 2
smlt 1
#VLAN CONFIGURATION #
config t
vlan members remove 1 1/47-1/48,2/1-2/2
vlan create 2 type port
vlan members remove 2 1/1-1/46,2/3-2/8,3/1-3/8
vlan members add 2 1/47-1/48,2/1-2/2
interface vlan 2
ip address 10.1.20.2 255.255.255.0
router ospf enable
router ospf
network 10.1.20.2
```

```
router vrrp ena
interface vlan 2
ip vrrp address 1 10.1.20.1
ip vrrp 1 enable
ip vrrp 1 backup-master enable
vlan create 3999 type port
vlan members remove 3999 1/1-1/47,2/3-2/8,3/1-3/8
vlan members add 3999 2/1-2/2
interface vlan 3999
ip address 2.1.1.1 255.255.255.0
#PORT CONFIGURATION - PHASE II #
config t
mlt spanning-tree 1 stp all learning disable
mlt spanning-tree 2 stp all learning disable
```

2. Configuration for R2

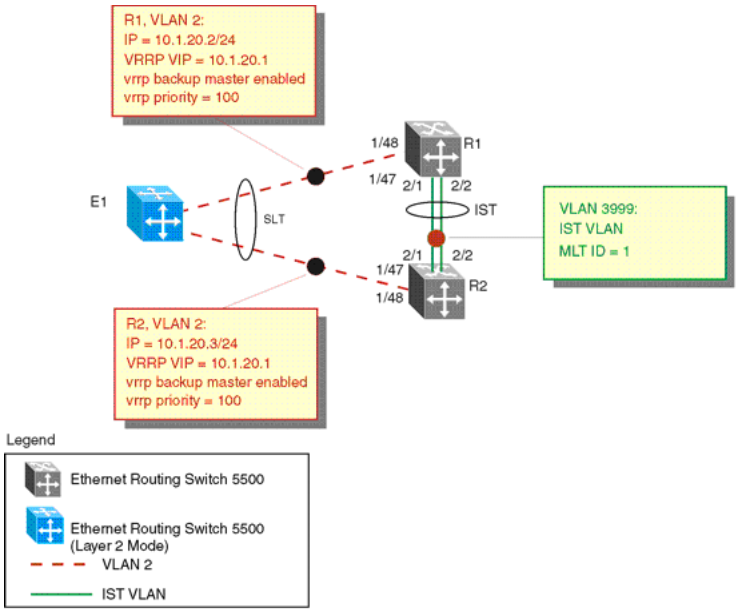
```
#MLT CONFIGURATION # config t
mlt 1 member 2/1-2/2
mlt 1 enable
vlan port 2/2-2/2 tagging enable
interface mlt 1
ist enable peer-ip 2.1.1.1 vlan 3999
mlt 2 member 1/48,1/47
mlt 2 enable
interface mlt 2
smlt 1
#VLAN CONFIGURATION #
config t
vlan members remove 1 1/47-1/48,2/1-2/2
vlan create 2 type port
vlan members remove 2 1/1-1/46,2/3-2/8,3/1-3/8
vlan members add 2 1/47-1/48,2/1-2/2
interface vlan 2
ip address 10.1.20.3 255.255.255.0
router ospf enable
router ospf
network 10.1.20.2
router vrrp ena
interface vlan 2
ip vrrp address 1 10.1.20.1
ip vrrp 1 enable
ip vrrp 1 backup-master enable
vlan create 3999 type port
vlan members remove 3999 1/1-1/47,2/3-2/8,3/1-3/8
vlan members add 3999 2/1-2/2
interface vlan 3999
ip address 2.1.1.2 255.255.255.0
#PORT CONFIGURATION - PHASE II #
config t
mlt spanning-tree 1 stp all learning disable
```

```
mlt spanning-tree 2 stp all learning disable
```

Configuring VRRP with SLT

The following illustration and configuration file examples demonstrate a VRRP configuration with SLT.

VRRP with SLT configuration



The following commands would recreate the above configuration:

1. Configuration for R1

```
#MLT CONFIGURATION #
config t
mlt 1 member 2/1-2/2
mlt 1 enable
vlan port 2/2-2/2 tagging enable
interface mlt 1
ist enable peer-ip 2.1.1.2 vlan 3999
interface fast-Ethernet 1/48
smlt 1
#VLAN CONFIGURATION #
config t
vlan members remove 1 1/48,2/1-2/2
vlan create 2 type port
vlan members remove 2 1/1-1/47,2/3-2/8,3/1-3/8
vlan members add 2 1/47,2/1-2/2
interface vlan 2
ip address 10.1.20.2 255.255.255.0
router ospf enable
router ospf
network 10.1.20.2
```

```
router vrrp ena
interface vlan 2
ip vrrp address 1 10.1.20.1
ip vrrp 1 enable
ip vrrp 1 backup-master enable
vlan create 3999 type port
vlan members remove 3999 1/1-1/47,2/3-2/8,3/1-3/8
vlan members add 3999 2/1-2/2
interface vlan 3999
ip address 2.1.1.1 255.255.255.0
#PORT CONFIGURATION - PHASE II #
config t
mlt spanning-tree 1 stp all learning disable
interface fast-Ethernet 1/48
spanning-tree stp 1 learning disable
```

2. Configuration for R2

```
#MLT CONFIGURATION #
config t
mlt 1 member 2/1-2/2
mlt 1 enable
vlan port 2/2-2/2 tagging enable
interface mlt 1
ist enable peer-ip 2.1.1.1 vlan 3999
interface fast-Ethernet 1/48
smlt 1
#VLAN CONFIGURATION #
config t
vlan members remove 1 1/48,2/1-2/2
vlan create 2 type port
vlan members remove 2 1/1-1/47,2/3-2/8,3/1-3/8
vlan members add 2 1/48,2/1-2/2
interface vlan 2
ip address 10.1.20.3 255.255.255.0
router ospf enable
router ospf
network 10.1.20.2
router vrrp ena
interface vlan 2
ip vrrp address 1 10.1.20.1
ip vrrp 1 enable
ip vrrp 1 backup-master enable
vlan create 3999 type port
vlan members remove 3999 1/1-1/47,2/3-2/8,3/1-3/8
vlan members add 3999 2/1-2/2
interface vlan 3999
ip address 2.1.1.2 255.255.255.0
#PORT CONFIGURATION - PHASE II #
config t
mlt spanning-tree 1 stp all learning disable
```

```
interface fast-Ethernet 1/48
spanning-tree stp 1 learning disable
```

Equal Cost Multipath (ECMP)

Equal Cost Multipath (ECMP) is an IP feature for load-balancing routed IP traffic across up to four equal-cost paths for each supported protocol. ECMP supports OSPF, RIP, and static routes. Some benefits of using ECMP:

- Supported protocols will rerun when an ECMP path fails, and the other configured paths will automatically take the load.
- Load sharing implies better use of network facilities.

ECMP is selected based on the source and destination IP address in the packet. The *hash_control* register has a *HASH_SELECT* field which is set to 5 (lower CRC-32).

R1 = CRC32 (SIP, DIP)

R2 = R1 & 0x1F(The Least Significant 5 bits are selected)

ecmp_index = R2 % (ecmp_count + 1)

> ***Note:*** The value *ecmp_count* above is zero-based in the hardware so if four paths are present then the value is three. This is why the value is *ecmp_count + 1*.

The ECMP traffic distribution algorithm is demonstrated in the following example:

Consider two network devices, Device 1 at the IP address 192.1.1.3 and Device 2 at 192.1.1.4. Device 1 send to Device 2 so that 192.1.1.3 is the source IP address (SIP) and 192.1.1.4 is the destination IP address (Device 2).

To calculate the CRC32 for the example source and destination IP address noted above, the following calculations would be made:

- CRC32 polynomial : x ^ 32 + x ^ 28 + x ^ 23 + x ^ 22 + x ^ 16 + x ^ 12 + x ^ 11 + x ^ 10 + x ^ 8 + x ^ 7 + x ^ 5 + x ^ 4 + x ^ 2 + x ^ 1 + 1
- R1 = CRC32 (0xc0010103, 0xc0010104) = 0xf474b549
- R2 = (0xf474b549 & 0x1f) = 9

If, for the purposes of this example, it is assumed that the ECMP count is 4 (hardware entries 0 though 3), the following calculation is then made:

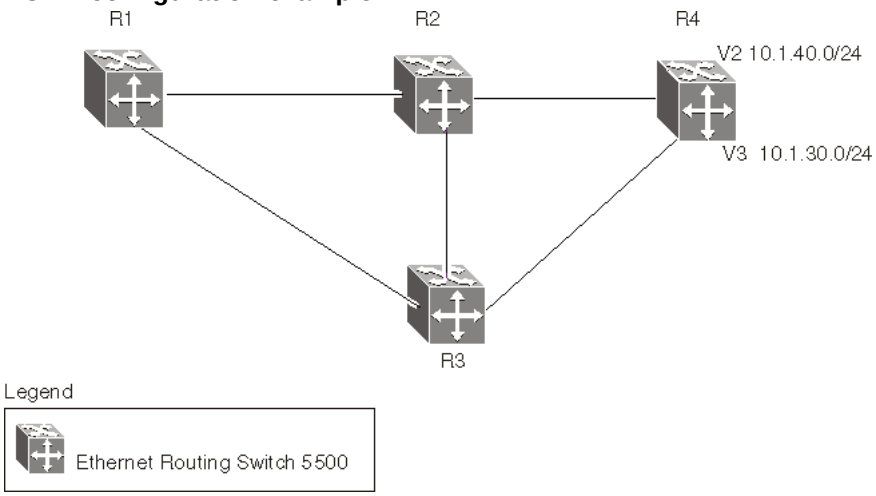
- ecmp_index = 9 % (4+1) = 1

This means that in this example, the second path at hardware index 1 in the ECMP table will be used.

In the configuration example illustrated below, the following command would enable two OSPF ECMP paths on router R1:

```
5530-24TFD(config)#ospf maximum-path 2
```

ECMP configuration example



Use the following commands to enable ECMP on each of the supported protocols:

- **OSPF**

  `ospf maximum-path <path_count>`

- **RIP**

  `rip maximum-path <path_count>`

- **Static Routes**

  `maximum-path <path_count>`

In all commands above, the **`<path_count>`** parameter represents the number of ECMP paths allotted. This is a value between 1 and 4. The default is 1.

Displaying the IP routing table

After ECMP configuration is complete, verify the ECMP paths in the routing table using the **`show ip route`** command. The following example displays the output for this command:

```
================================================================================
                                Ip Route
================================================================================
DST             MASK            NEXT            COST VLAN PORT PROT TYPE PRF
--------------------------------------------------------------------------------
0.0.0.0         0.0.0.0         10.100.111.1    10   1    19    S    IB   5
3.3.3.0         255.255.255.0   3.3.3.1         1    2     -    C    DB   0
4.4.4.0         255.255.255.0   4.4.4.1         1    2     -    C    DB   0
5.5.5.0         255.255.255.0   5.5.5.1         1    2     -    C    DB   0
10.10.10.0      255.255.255.0   10.10.10.1      1    5     -    C    DB   0
10.100.111.0    255.255.255.0   10.100.111.200  1    1     -    C    DB   0
Total Routes: 6
--------------------------------------------------------------------------------
TYPE Legend: I=Indirect Route, D=Direct Route, A=Alternative Route,
B=Best Route,E=Ecmp Route, U=Unresolved Route, N=Not in HW
```

Paths shown with the letter **E** in the **TYPE** column are designated equal-cost paths. In this example, two routes to IP address 10.1.40.0 and two routes to IP address 10.1.30.0 are displayed.

Displaying global ECMP configuration

To confirm global ECMP configuration, use the show ecmp command. A sample output from this command is displayed below:

```
5530-24TFD# show ecmp
Protocol      MAX-PATH
--------      --------
static:           1
rip:              2
ospf:             4
```

IP routing configuration using the Java Device Manager

This section describes the procedures for IP routing configuration using the Java Device Manager (JDM).

Layer 3 routable VLANs

The Nortel Ethernet Routing Switch 5500 Series are Layer 3 (L3) switches. This means that a regular L2 VLAN becomes a routable L3 VLAN if an IP address and MAC address are attached to the VLAN. When routing is enabled in L3 mode, every L3 VLAN is capable of routing as well as carrying the management traffic. The user can use any L3 VLAN instead of the Management VLAN to manage the switch.

This section covers the functionality in the Java Device Manager used to make Layer 3 Routable VLANs possible.

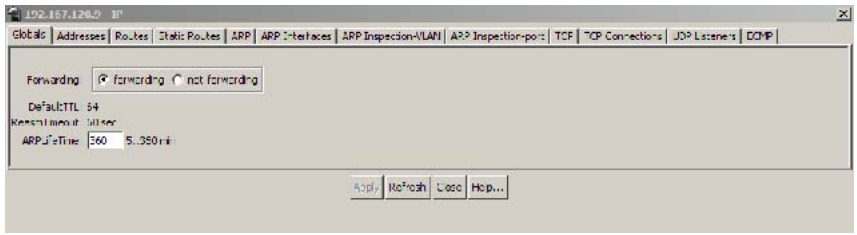
Creating a Layer 3 routable VLAN

Note: The creation of a Management VLAN in the JDM requires the assignment of an IP address to a VLAN. Ensure that IP forwarding is turned on before proceeding.

To enable IP forwarding on the switch, follow this procedure:

Step	Action
1	Open the **IP** dialog by selecting **IP Routing > IP** from the Device Manager menu. The **IP** dialog opens with the **Globals** tab selected. This tab is illustrated below.

IP dialog - Globals tab



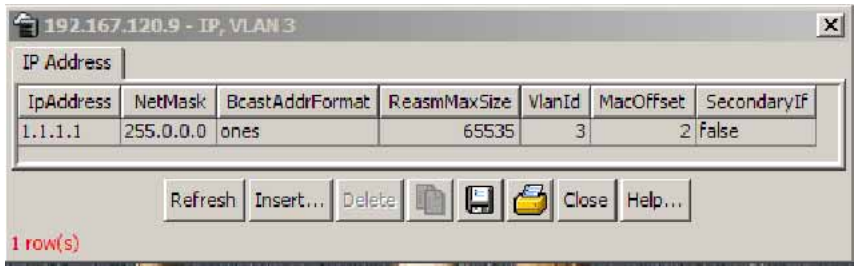
2	In the **Forwarding** section, select the **forwarding** option.
3	Click **Apply**.

—End—

With IP forwarding enabled on the switch, the creation of a Layer 3 Routable VLAN can proceed. To create a Layer 3 Routable VLAN, follow this procedure:

Step	Action
1	Open the **VLANs** screen by selecting **VLAN > VLANs** from the JDM menu.
2	Select the VLAN for Management VLAN assignment.
3	Click **IP**. The **IP VLAN** screen opens with the **IP Address** tab selected. This screen and tab are illustrated below.

IP VLAN screen



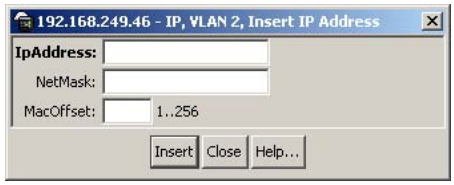
The following table describes the IP Address tab fields.

IP Address tab fields

Field	Description
IpAddress	The IP address associated with the selected VLAN.
NetMask	The subnet mask address.
BcastAddrFormat	The IP broadcast address format used on this interface.
ReasmMaxSize	The size of the largest IP datagram which this entity can reassemble from fragmented incoming IP datagrams received on this interface.
VlanId	The VLAN number. A value of -1 indicates that the VLAN ID is ignored.
MacOffset	Used to translate the IP address into a MAC address. The valid range is 1--256.
SecondaryIf	Indicates whether or not this entry corresponds to a secondary interface. If the value is **false**, then this is the primary IP address, if the value is **true**, then this is a secondary IP address. ***Note:*** You can assign 1 primary IP address and up to 8 secondary IP addresses to a VLAN.

4 Click **Insert**. The Insert IP Address screen opens. This screen is illustrated below.

Insert IP Address screen



5 Type the **IP Address**, **Subnet Mask**, and **Mac Address Offset** in the fields provided.

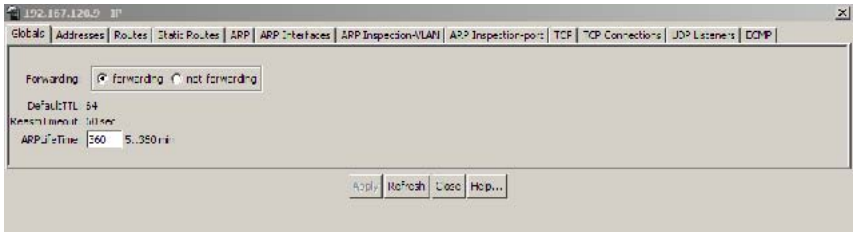
6 Click **Insert**.

—End—

IP routing

IP routing tasks are performed in the JDM using the **IP** screen. To open the **IP** screen, select **IP Routing > IP** from the menu. This screen is illustrated below.

IP screen



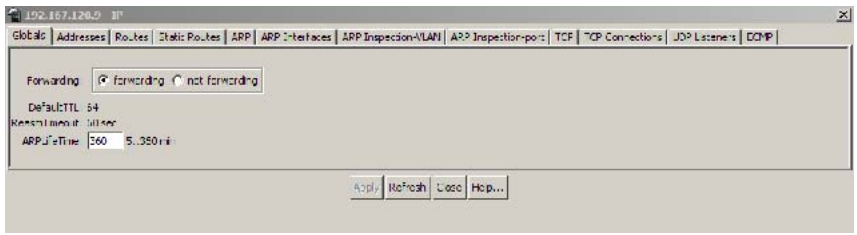
This section outlines the various tabs on this screen and their use in IP routing configuration.

Globals tab

The **Globals** tab is used to configure global IP routing information. To configure this information, follow this procedure:

Step	Action

1 Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **Globals** tab. This tab is illustrated below.



2 In the fields provided, enter the necessary configuration information. The following table outlines the fields on this tab.

Globals tab fields

Field	Description
Forwarding	Indicates whether the switch is forwarding datagrams received by it but not addressed to it. Generally, IP routers forward datagrams but IP hosts do not (except those source-routed through the host).
DefaultTTL	Default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. Default value is 64.
ReasmTimeout	Maximum number of seconds that received fragments are held while they await reassembly at this entity. Default value is 60.
ARPLifeTime	The lifetime in minutes of an ARP entry within the system.

3 Click **Apply**.

—End—

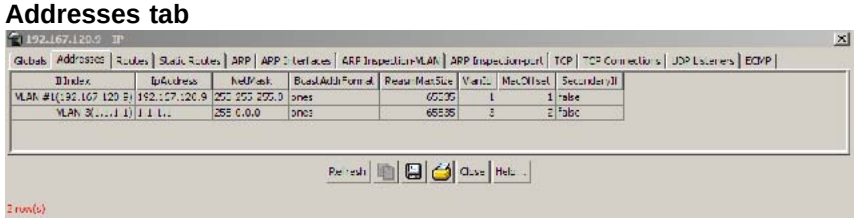
Addresses tab

The **Addresses** tab displays IP information for the switch. To view the information on this tab, follow this procedure:

Step Action

1 Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **Addresses** tab. This tab is illustrated below.

Addresses tab



The **Addresses** tab is a read-only tab. Click **Refresh** to immediately refresh the information it displays. The fields on this tab are outlined in the following table.

Addresses tab fields

Field	Description
IfIndex	The port number or VLAN ID.
IpAddress	The device IP address.
NetMask	The subnet mask address.
BcastAddrFormat	The IP broadcast address used.
ReasmMaxSize	The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.
VlanId	The VLAN number. A value of -1 indicates that the VLAN ID is ignored.
MacOffset	Used to calculate the offset of the VLAN MAC from the switch MAC.
SecondaryIf	The SecondaryIf field is set to **True** if the VLAN IP address is a secondary IP address and **False** if the IP address for the VLAN is the primary IP address.

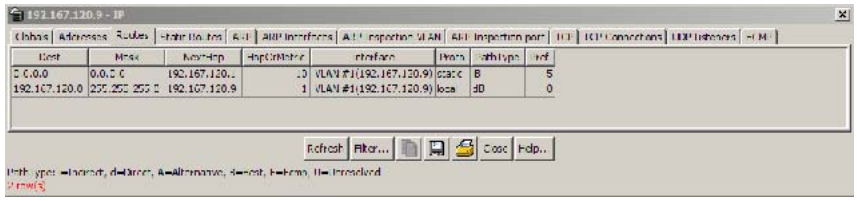
—End—

Routes tab

The **Routes** tab lists the different routes (dynamic or static) known to the switch. To view the known routes, perform the following procedure:

Step	Action
1	Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **Routes** tab. This tab is illustrated below.

IP dialog- Routes tab



Step	Action
2	Using the fields provided, view the information provided on switch routes. The fields on this tab are described in the following table.

Routes tab fields

Field	Description
Dest	The destination address of the route.
Mask	The subnet mask used by the route destination.
NextHop	The next hop in the listed route.
HopOrMetric	The OSPF hop count or metric associated with the route.
Interface	The interface associated with the route.
Proto	The protocol associated with the route.
PathType	The route path type.
Pref	The preference value associated with the route.

—End—

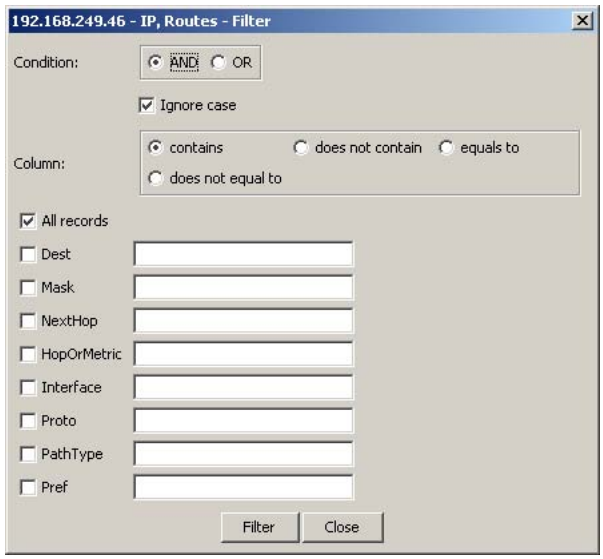
Note: Routes will not be displayed until at least one port in the VLAN has link.

The route list can be updated by clicking the Refresh button. The route list can also be filtered. This is described below.

Filtering route information

The **Routes** tab can be filtered to display only the desired switch routes. Use the following procedure to filter the **Routes** tab:

Step	Action
1	With the **Routes** tab open, click the **Filter** button. The **Filter** dialog is displayed. This dialog is illustrated below.



2 Using the fields provided, set the filter for the tab. These fields are described in the following table.

Filter dialog fields

Field	Description
Condition	When using multiple filter expressions on the tab, this is the condition that is used to join them together.
Ignore Case	Denotes whether filters are case sensitive or insensitive.
Column	Denotes the type of criteria that will be applied to values used for filtering.
All Records	Select this check box to clear any filters and display all rows.
Dest	Select this check box and enter a value to filter on the route destination value.
Mask	Select this check box and enter a value to filter on the route destination subnet mask value.
NextHop	Select this check box and enter a value to filter on the route next hop value.
HopOrMetric	Select this check box and enter a value to filter on the hop count or metric of the route.
Interface	Select this check box and enter a value to filter on the route's associated interface.
Proto	Select this check box and enter a value to filter on the route protocol.

PathType	Select this check box and enter a value to filter on the route path type.
Pref	Select this check box and enter a value to filter on the route preference value.

3 Click **Filter**.

—End—

The tab will now be filtered on the criteria specified.

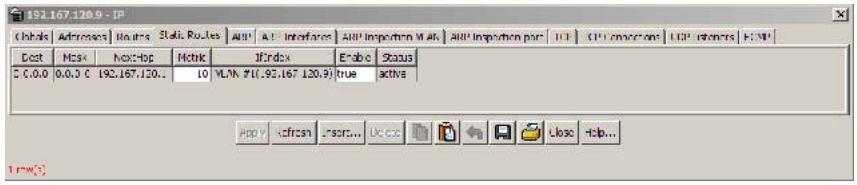
Static Routes tab

The **Static Routes** tab is used to configure static routes for the switch. To configure a static route with this tab, follow this procedure:

Step	Action

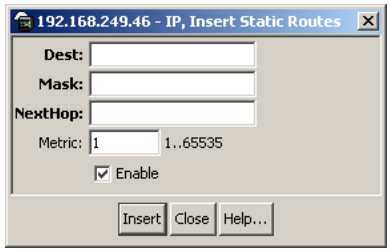
1 Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **Static Routes** tab. This tab is illustrated below.

Static Routes tab



2 Click **Insert**. The **Insert Static Route** screen opens. This screen is illustrated below.

Insert Static Route screen



3 In the fields provided, enter the information for the new static route. The following table outlines the fields on this screen.

Insert Static Route fields

Field	Description
Dest	The destination IP address of the route. 0.0.0.0 is considered the default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.
Mask	The destination mask of the route.
NextHop	The IP address of the next hop of this route. In the case of a route bound to an interface that is realized through a broadcast media, the value of this field is the agent IP address on that interface.
Metric	This field represents the cost of the static route. It is used to choose the best route (the one with the smallest cost) to a certain destination. This field has a range of 1 to 65535. If this metric is not used, the value is set to -1.
Enable	Enable the new static route.

4 Click **Insert**. The new static route is displayed on the **Static Routes** tab.

—End—

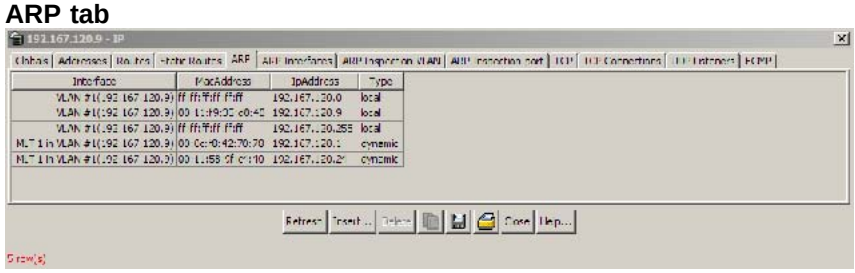
ARP tab

The **ARP** tab is used to configure Address Resolution Protocol (ARP) entries for the switch. To configure the **ARP** tab, follow this procedure:

Step	Action

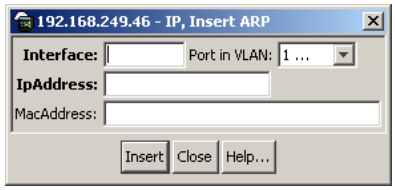
1 Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **ARP** tab. This tab is illustrated below.

ARP tab



2 Click **Insert**. The **Insert ARP Entry** screen opens. This screen is illustrated below.

Insert ARP Entry screen



3 To determine the interface and VLAN to use for the ARP entry, do the following:

a. Select a VLAN from the **Port in VLAN** drop down list.

b. Using the provided dialog, select the ports that will be used in this entry.

c. The **Interface** field will be populated with the appropriate VLAN / interface information.

4 In the fields provided, enter the remainder of the required information for the new ARP entry. These fields are outlined in the following table.

Insert ARP Entry fields

Field	Description
MacAddress	The unique hardware address of the device.
IpAddress	The IP address of the device used to represent a point of attachment in a TCP/IP internetwork.

5 Click **Insert**. The **ARP** tab is displayed with the new entry.

—End—

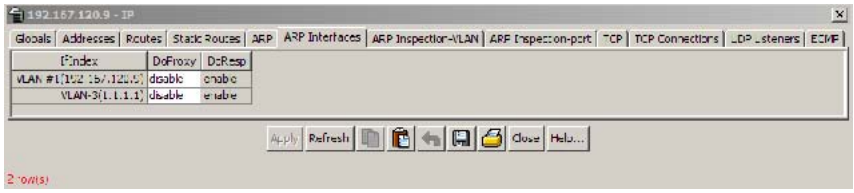
ARP Interfaces tab

The **ARP Interfaces** tab is used to configure proxy ARP on the switch. Proxy ARP allows the switch to respond to an ARP request from a locally attached host (or end station) for a remote destination.

To configure proxy ARP, use the following procedure:

Step	Action
1	Select **IP Routing > IP** from the Device Manager menu. The **IP** dialog opens with the **Globals** tab selected.
2	Select the **ARP Interfaces** tab. This tab is illustrated below.

IP screen - ARP Interfaces tab



3 Using the provided fields, configure proxy ARP. These fields are outlined in the following table.

ARP Interfaces tab fields

Field	Description
IfIndex	The index of the configured switch interface.
DoProxy	Enable or disable proxy ARP on the interface.
DoResp	Enable or disable the sending of ARP responses on the specified interface.

4 Click **Apply**.

—End—

ARP Inspection VLAN tab

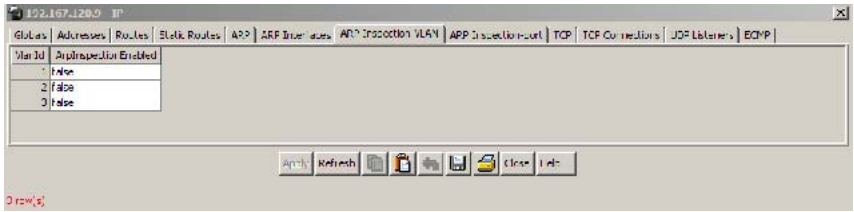
To view and change ARP inspection status for VLANs, use the following procedure:

Step	Action

1 From the Device Manager, select **IP Routing > IP**. The **IP** window appears.

2 Select the **ARP Inspection-VLAN** tab. The **ARP Inspection-VLAN** window appears.

ARP Inspection-VLAN tab



3 To change the ARP Inspection status for a VLAN, select the VLAN.

4 Double click the ArpInspectionEnabled field for the VLAN.

5 Select **true** to enable ARP Inspection-VLAN or **false**to disable ARP Inspection-VLAN.

6 Click **Apply**.

—End—

ARP Inspection port tab

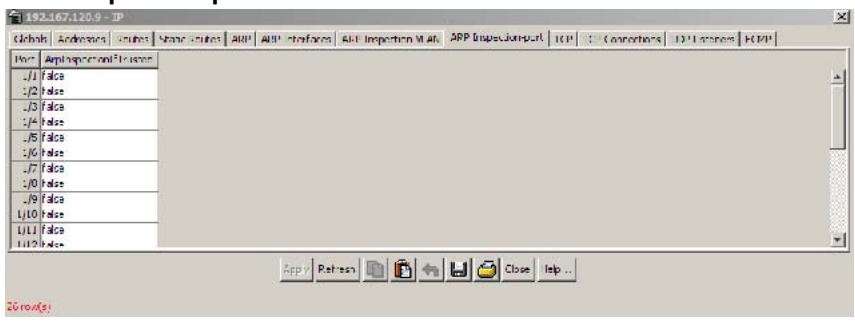
To view and change ARP inspection status for ports, use the following procedure:

Step	Action

1 From the Device Manager, select **IP Routing > IP**. The **IP** window appears.

2 Select the **ARP Inspection-port** tab. The **ARP Inspection-port** window appears.

ARP Inspection-port tab



3 To change the ARP Inspection status for a port, select the port.

4 Double click the ArpInspectionIfTrusted field for the port.

5 Select **true** enable ARP Inspection or **false**to disable ARP Inspection.

6 Click **Apply**.

—End—

Note: ArpInspectionIfTrusted controls whether or not the interface is trusted for ARP inspection.

TCP tab

The **TCP** tab displays Transmission Control Protocol (TCP) information for the switch. This is a read-only tab. To view information on the **TCP** tab, follow this procedure:

Step	Action

1 Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **TCP** tab. This tab is illustrated below.

TCP tab

2 Click **Refresh** to immediately refresh the information this tab displays.

The following table outlines the fields on this tab.

TCP tab fields

Field	Description
RtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
RtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
RtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
MaxConn	The limit on the total number of TCP connections that the entity can support. In entities where the maximum number of connections is dynamic, this object contains the value -1.

—End—

TCP Connections tab

This tab displays information on the current TCP connections the switch maintains. This tab is read-only. To view information on this tab, follow this procedure:

Step	Action

1 Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **TCP Connections** tab. This tab is illustrated below.

TCP Connections tab

2 Click **Refresh** to immediately refresh the information this tab displays.

The following table describes the fields on this tab.

TCP Connections tab fields

Field	Description
LocalAddress	The local IP address for this TCP connection. In the case of a connection in the listen state, which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.
LocalPort	The local port number for this TCP connection.
RemAddress	The remote IP address for this TCP connection.
RemPort	The remote port number for this TCP connection.
State	The state of this TCP connection.

—End—

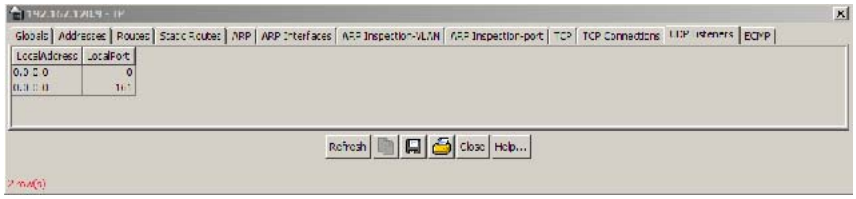
UDP Listeners tab

This tab displays information on the UDP listeners currently maintained by the switch. This tab is read-only. To view the information on this tab, follow this procedure:

Step	Action

1 Open the **IP** screen by selecting **IP Routing > IP** from the menu. Select the **UDP Listeners** tab. This tab is illustrated below.

UDP Listeners tab



2 Click **Refresh** to immediately refresh the information displayed.

The following table outlines the fields on this tab.

UDP Listeners tab fields

Field	Description
LocalAddress	The local IP address for this UDP listener. In the case of a UDP listener that accepts datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.
LocalPort	The local port number for this UDP listener.

—End—

ECMP tab

The **ECMP** tab is used to configure the Equal Cost Multipath (ECMP) feature on the switch.

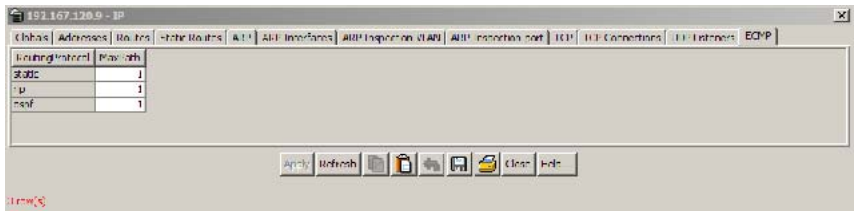
To configure ECMP, use the following procedure:

Step	Action

1 Select **IP Routing > IP** from the Device Manager menu. The **IP** dialog opens with the **Globals** tab selected

2 Select the **ECMP** tab. This tab is illustrated below.

IP dialog - ECMP tab



3 Using the provided fields, configure ECMP. These fields are outlined in the following table.

ECMP tab fields

Field	Description
RoutingProtocol	The routing protocol to be configured.
MaxPath	The maximum number of ECMP paths assigned to the protocol.

4 Click **Apply**.

—End—

Routing Information Protocol (RIP) configuration

This section describes the Java Device Manager procedures used to configure and manage the Routing Information Protocol (RIP) on the Nortel Ethernet Routing Switch 5500 Series. RIP is a distance vector protocol used to dynamically discover network routes based on information passed between routers in the network. RIP is useful in network environments where using static route administration would be difficult.

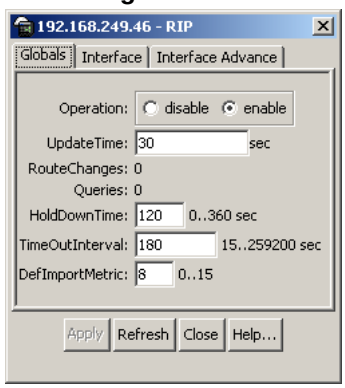
Global RIP configuration

Global RIP configuration is used to configure the RIP parameters that will apply to all active RIP interfaces. To configure global parameters, follow this procedure:

Step	Action

1 Select **IP Routing > RIP** from the Device Manager menu. The **RIP** dialog is opened with the **Globals** tab selected. This tab is illustrated below.

RIP dialog - Globals tab



2 Using the fields provided, configure the global RIP parameters. The following table describes these parameters.

Globals tab fields

Field	Description
Operation	Enables or disables the operation of RIP on all interfaces. The default is disabled.
UpdateTime	The time interval between RIP updates on all interfaces. It is a global parameter for the box; that is, it applies to all interfaces and cannot be set individually for each interface. The default is 30 seconds.
RouteChanges	The number of route changes made to the IP Route Database by RIP; does not include the refresh of a route's age.
Queries	The number of responses sent to RIP queries from other systems.
HoldDownTime	Sets the length of time that RIP will continue to advertise a network after determining it is unreachable. The range is 0 to 360 seconds. The default is 120 seconds.
TimeOutInterval	The time out interval between RIP update and all interfaces.
DefImportMetric	Sets the value of the default import metric to import a route into a RIP domain. For announcing OSPF internal routes into a RIP domain, if the policy does not specify a metric value, the default import metric should be used. For OSPF external routes, the external cost is used.

3 Click **Apply**.

—End—

RIP interface configuration

RIP interface configuration is used to tailor RIP to the individual interfaces. To configure a RIP interface, perform the following procedure:

Step	Action

1 Select **IP Routing > RIP** from the Device Manager menu. The **RIP** dialog is opened. Select the **Interface** tab. This tab is illustrated below.

RIP dialog - Interface tab

2 Using the fields provided, configure the interface. The following table describes these fields.

Interface tab fields

Field	Description
Address	The IP address of the RIP interface. This field is for organizational purposes only and cannot be edited.
Send	Sets the RIP version sent on this interface. The following values are valid: • doNotSend - No RIP updates sent on this interface. • ripVersion1 - RIP updates compliant with RFC 1058. • rip1Compatible - Broadcasts RIPv2 updates using RFC 1058 route subsumption rules. • ripVersion2 - Multicasting RIPv2 updates. The default is rip1Compatible.
Receive	Sets the RIP version received on this interface: rip1, rip2, or rip1OrRip2 The default is rip1OrRip2. Note that rip2 and rip1OrRip2 imply reception of multicast packets.

3 Click **Apply**.

—End—

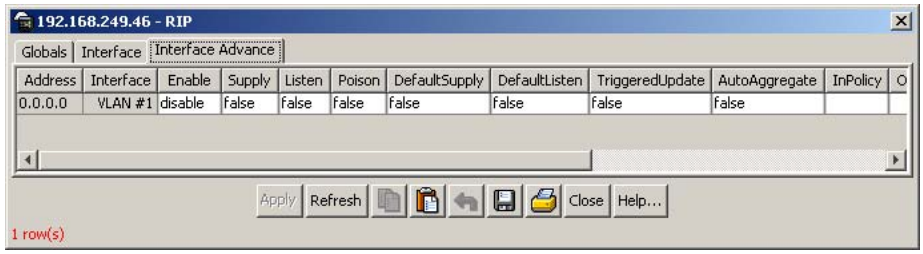
Advanced RIP interface configuration

Advanced RIP interface configuration is used to fine tune and further configure a RIP interface. To configure advanced RIP interface options, follow this procedure:

Step	Action

1 Select **IP Routing > RIP** from the Device Manager menu. The **RIP** dialog is opened. Select the **Interface Advance** tab. This tab is illustrated below.

RIP dialog - Interface Advance tab



2 Using the fields provided, configure the advanced RIP features. These fields are described in the following table.

Interface Advance tab fields

Field	Description
Address	The IP address of the RIP interface. This field is for organizational purposes only and cannot be edited.
Interface	The switch interface that corresponds to the listed IP address.
Enable	Enables or disables RIP on this interface.
Supply	Determines whether this interface supplies RIP advertisements.
Listen	Determines whether this interface listens for RIP advertisements.
Poison	Enables or disables poison reverse on this interface.
DefaultSupply	Determines whether this interface advertises default routes.

DefaultListen	Determines whether this interface listens for default route advertisements.
TriggeredUpdate	Enables or disables triggered updates on this interface.
AutoAggregate	Enables or disables auto aggregation on this interface.
InPolicy	Associates a previously configured switch policy with this interface for use as an in policy.
OutPolicy	Associates a previously configured switch policy with this interface for use as an out policy.
Cost	The cost associated with this interface.
HoldDownTime	Sets the holddown timer for this interface. This is an integer value in seconds between 0 and 360.
TimeoutInterval	Sets the timeout interval for this interface. This is an integer value between 15 and 259200.
ProxyAnnounceFlag	Enables or disables proxy announcements on this interface.

3 Click **Apply**.

—End—

RIP Statistics

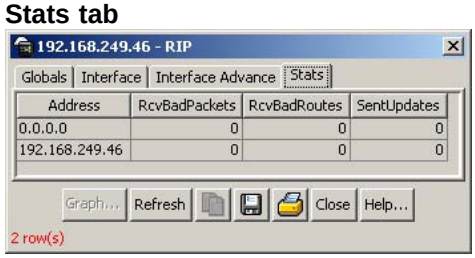
The **Stats** tab provides statistical information about the currently configured RIP interfaces. To view these RIP statistics, follow this procedure:

Step	Action

1 Select **IP Routing > RIP** from the Device Manager menu. The **RIP** dialog opens with the **Globals** tab selected.

2 Select the **Stats** tab. This tab is illustrated below.

Stats tab



3 RIP statistics for the configured interfaces are displayed. The fields on this tab are outlined in the following table.

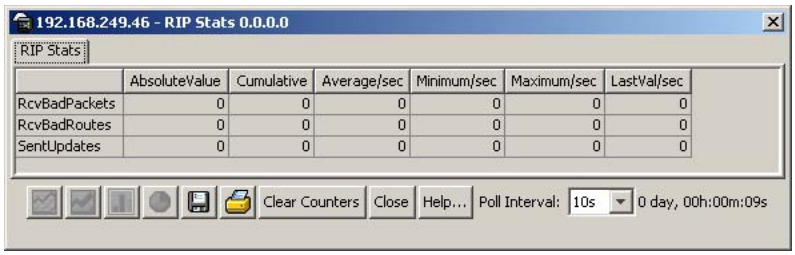
Stats tab fields

Field	Description
Address	The RIP interface address.
RcvBadPackets	The number of RIP response packets received by the interface that have been discarded.
RcvBadRoutes	The number of RIP routes received by the interface that have been ignored.
SentUpdates	The number of triggered RIP updates actually sent on this interface. This does not include full updates sent containing new information.

—End—

To graph these statistics, select a row from the **Stats** tab and click the **Graph** button. A new dialog will open with the statistics for the selected interface. This dialog is illustrated below.

RIP Stats Graph dialog



Select a graph type by clicking the appropriate graphing button.

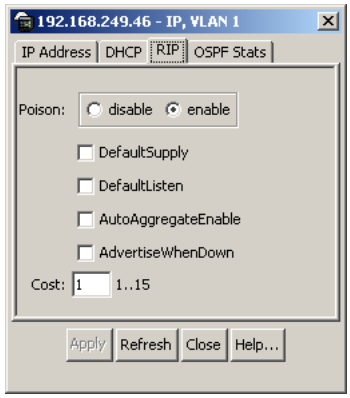
VLAN RIP configuration

The **RIP** tab of the **IP VLAN** screen is used to configure RIP parameters for the interface.

To configure VLAN RIP parameters, use the following procedure:

Step	Action
1	Select **VLAN > VLANs** from the Device Manager menu. The **VLAN** dialog opens with the **Basic** tab selected.
2	On the **Basic** tab, select an interface and click the **IP** button.
3	The **IP VLAN** screen opens with the **IP Address** tab selected. Select the **RIP** tab. This tab is illustrated below.

IP VLAN screen - RIP tab



4 Using the provided fields, configure the interface RIP parameters. These fields are outlined in the following table.

RIP tab fields

Field	Description
Poison	Determines whether or not poison reverse is implemented on this interface.
DefaultSupply	Determines whether or not the interface implements the default supply mechanism.
DefaultListen	Determines whether or not the interface implements the default listen mechanism.
AutoAggregateEnable	Determines whether or not auto aggregation is enabled on this interface.
AdvertiseWhenDown	Determines whether or not this interface will advertise even when non-operational.
Cost	The cost associated with this interface.

5 Click **Apply**.

—End—

Open Shortest Path First (OSPF) configuration

The Open Shortest Path First (OSPF) Protocol is an Interior Gateway Protocol (IGP) that distributes routing information between routers belonging to a single *autonomous system* (AS). Intended for use in large networks, OSPF is a link-state protocol which supports IP subnetting and the tagging of externally-derived routing information.

This section describes the configuration of OSPF on the switch using the Java Device Manager.

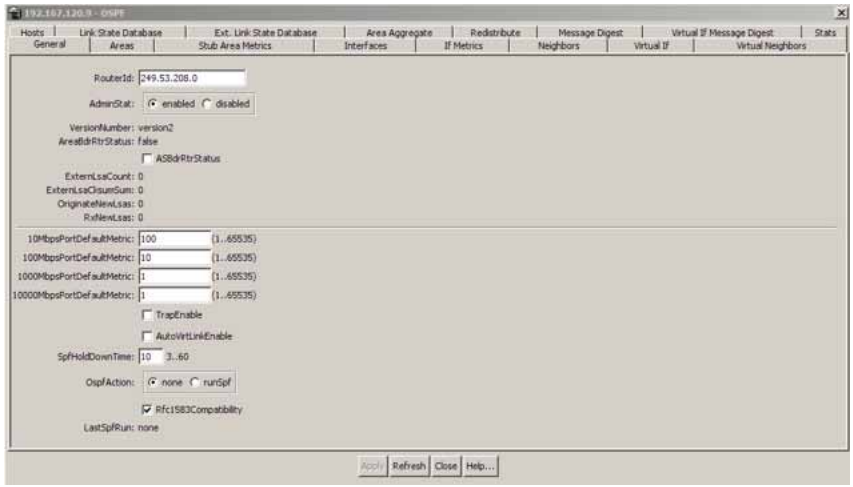
Global OSPF configuration

The **General** tab of the **OSPF** dialog is used to configure global OSPF parameters. To configure these parameters, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open with the **General** tab selected. This tab is illustrated below.

OSPF dialog - General tab



2 Using the fields provided, configure the global OSPF parameters. These fields are described in the following table.

General tab fields

Field	Description
RouterId	The unique ID of the router in the Autonomous System.
AdminStat	The administrative status of OSPF on the router.
VersionNumber	The current OSPF version number.
AreaBrdRtrStatus	Denotes whether this router is an Area Border Router.
ASBrdRtrStatus	Denotes whether this router is an Autonomous System Border Router.

Field	Description
ExternLsaCount	The number of external (link state type 5) link-state advertisements in the link state database.
ExternLsaCksumSum	The sum of the link state checksums of the external link state advertisements contained in the link state database. This sum can be used to determine if there has been a change in a router's link state database and to compare the link state database of two routers.
OriginateNewLsas	The number of new link state advertisements that have been originated. This number is incremented each time the router originates a new link state advertisement.
RxNewLsas	The number of link state advertisements received determined to be new instantiations. This number does not include newer instantiations of self-originated link state advertisements.
10MbpsPortDefaultMetric	The default metric of a 10 Mbps port. This is an integer value between 1 and 65535.
100MbpsPortDefaultMetric	The default metric of a 100 Mbps port. This is an integer value between 1 and 65535.
1000MbpsPortDefaultMetric	The default metric of a 1000 Mbps port. This is an integer value between 1 and 65535.
10000MbpsPortDefaultMetric	The default metric of a 10000 Mbps port. This is an integer value between 1 and 65535.
TrapEnable	Indicates whether OSPF traps should be sent.
AutoVirtLinkEnable	Indicates status of OSPF automatic Virtual Link. The default setting is disabled.
SpfHoldDownTime	The SPF Hold Down Timer value is an integer between 3 and 60. The SPF will run, at most, once per hold down timer value.
OspfAction	An immediate OSPF action to take. Select **runSpf** and click **Apply** to do an immediate SPF run.

Field	Description
Rfc1583Compatibility	Controls the preference rules used when choosing among multiple Autonomous System external link state advertisements advertising the same destination. When this is enabled, the preference rule will be the same as specified by RFC 1583. When disabled, the new preference rule, as described in RFC 2328, will be applicable. This potentially prevents the routing loops when Autonomous System external link state advertisements for the same destination have been originated from different areas.
LastSpfRun	Used to indicate the time the last SPF calculation was done.

3 Click **Apply**.

—End—

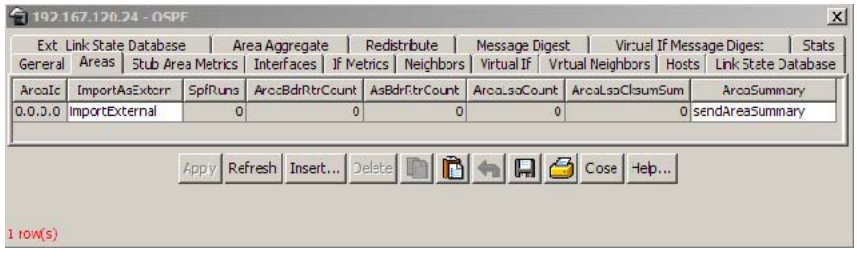
OSPF area configuration

The **Areas** tab of the **OSPF** dialog is used to configure OSPF area parameters. To configure these parameters, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Areas** tab. This tab is illustrated below.

OSPF dialog - Areas tab



2 Using the fields provided, configure the existing OSPF areas. These fields are described in the table below.

Areas tab fields

Field	Description
AreaId	The area's unique identifier. Area ID *0.0.0.0* is used for the OSPF backbone.
ImportAsExtern	The area's support for importing Autonomous System external link state advertisements. The options available are: importExternal, importNoExternal, and importNssa.
SpfRuns	The number of times that the intra-area route table has been calculated using this area link state database.
AreaBdrRtrCount	The total number of Area Border Routers reachable within this area. This is initially zero and is calculated in each SPF pass.
AsBdrRtrCount	The total number of Autonomous System Border Routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AreaLsaCount	The total number of link state advertisements in this area's link state database, excluding Autonomous System external link state advertisements.
AreaLsaCksumSum	The sum of the link state advertisements' checksums contained in this area's link state database. This sum excludes external (link state type 5) link state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link state database of two routers.
AreaSummary	Controls the import of summary link state advertisements into stub areas. It has no effect on other areas. If the value is noAreaSummary, the router will neither originate nor propagate summary link state advertisements into the stub area. If the value is sendAreaSummary, the router will both summarize and propagate summary link state advertisements.

3 Click **Apply**.

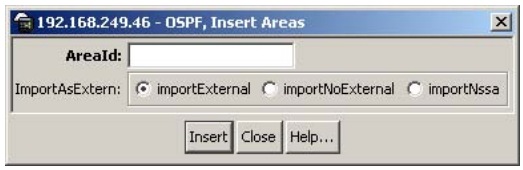
—End—

OSPF area creation

The Areas tab can also be used to create a new OSPF area. To create a new OSPF area, follow this procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Areas** tab. This tab is illustrated above.
2	Click **Insert**.
3	The **Insert Areas** dialog opens. This dialog is illustrated below.

Insert Areas dialog



4	Using the fields provided, create the new area. These fields are described in the following table.

Insert Areas dialog fields

Field	Description
AreaId	The area's unique identifier. Area ID *0.0.0.0* is used for the OSPF backbone.
ImportAsExtern	The area's support for importing Autonomous System external link state advertisements. The options available in this drop down list are: importExternal, importNoExternal, and importNssa.

5	Click **Insert**.

—End—

OSPF area deletion

To delete an OSPF area, use the following procedure.

Deleting an OSPF area

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog opens.
2	Select the **Areas** tab.
3	Select an **AreaID** to delete.
4	Click **Delete**.

—End—

Stub Area Metrics configuration

The **Stub Area Metrics** tab of the **OSPF** dialog is used to configure stub area metrics associated with different types of service. To configure these parameters, use the following procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Stub Area Metrics** tab. This tab is illustrated below.

OSPF dialog - Stub Area Metrics tab

Step	Action
2	Using the fields provided, configure the stub area metrics. These fields are described in the table below.

Stub Area Metrics tab fields

Field	Description
AreaId	The unique ID of the stub area.
TOS	The Type of Service associated with the metric.
Metric	The metric value applied to the indicated type of service. By default, this equals the least metric at the type of service among the interfaces to other areas.
Status	Displays the status of the entry; **Active** or **Not Active**. This field is read-only.

3 Click **Apply**.

—End—

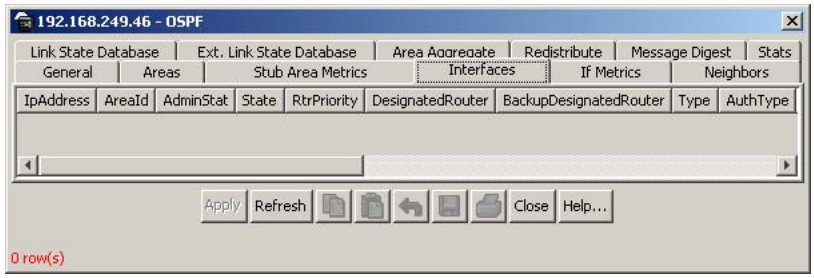
Interface configuration

The **Interfaces** tab of the **OSPF** dialog is used to configure OSPF interfaces. To configure OSPF interfaces, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Interfaces** tab. This tab is illustrated below.

OSPF dialog - Interfaces tab



2 Using the fields provided, configure the OSPF interface. These fields are described in the table below.

Interfaces tab fields

Field	Description
IpAddress	The IP address of the OSPF interface.
AreaId	The unique ID of the area to which the interface connects. Area ID 0.0.0.0 indicates the OSPF backbone.
AdminStat	The administrative status of the OSPF interface.
State	Correct DR state of the OSPF interface (DR, BDR, OtherDR).

Field	Description
RtrPriority	The priority of the interface. Used in multi-access networks, this field is used in the designated router election algorithm. The value 0 signifies that the router is not eligible to become the designated router on this network. In the event of a tie in this value, routers will use their Router ID as a tie breaker. This is an integer value between 0 and 255.
DesignatedRouter	The IP address of the Designated Router.
BackupDesignatedRouter	The IP address of the Backup Designated Router.
Type	The OSPF interface type. The options available are: broadcast or passive.
AuthType	The interface authentication type. The options available are: none, simplePassword, or md5.
AuthKey	The interface authentication key. This key is for when AuthType is simplePassword.
PrimaryMd5Key	The MD5 primary key if it exists. Otherwise this field will display 0.
HelloInterval	The interval in seconds between the Hello packets sent by the router on this interface. This value must be the same for all routers attached to a common network. This is an integer value between 1 and 65535.
TransitDelay	The estimated number of seconds it takes to transmit a link state update packet over this interface. This is an integer value between 0 and 3600.
RetransInterval	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. This value is also used when retransmitting database description and link state request packets. This is an integer value between 0 and 3600.

Field	Description
RtrDeadInterval	The number of seconds that a router's Hello packets have not been transmitted before the router neighbors declare it down. This value should be some multiple of the Hello interval and must be the same for all routers attached to the common network. This is an integer value between 0 and 2147483647 and must be multiple of the **HelloInterval** value.
PollInterval	The number of seconds allocated between polls.
AdvertiseWhenDown	Indicates if this interface advertises even when it is non-operational.
MtuIgnore	Indicates whether the MTU value is ignored.
Events	The number of times this OSPF interface has changed its state or an error has occurred.

3 Click **Apply**.

—End—

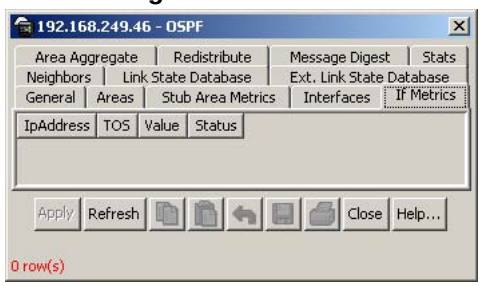
Interface Metric configuration

The **If Metrics** tab of the **OSPF** dialog is used to configure OSPF interface metrics. To configure OSPF interface metrics, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **If Metrics** tab. This tab is illustrated below.

OSPF dialog - If Metrics tab



2 Using the fields provided, configure the interface metrics. These fields are described in the table below.

If Metrics tab fields

Field	Description
IpAddress	The IP address of the interface.
TOS	The Type of Service associated with the metric.
Value	The value advertized to other areas indicating the distance from the OSPF router to any network in the range. This is an integer value between 0 and 65535.
Status	Displays the status of the entry; **Active** or **Not Active**. This field is read-only.

3 Click **Apply**.

—End—

Neighbor information

The **Neighbors** tab of the **OSPF** dialog is used to view OSPF neighbor information. To view OSPF neighbors, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Neighbors** tab. This tab is illustrated below.

OSPF dialog - Neighbors tab

2 Using the fields provided, view the OSPF neighbor information. These fields are explained in the table below.

Neighbor tab fields

Field	Description
IpAddr	The IP address this neighbor is using as an IP source address. On addressless links, this will not be represented as *0.0.0.0* but as the address of another of the neighbor's interfaces.
AddressLessIndex	The corresponding value of the interface index on addressless links. This value is zero for interfaces having an IP address.
Router	The unique ID of the neighboring router in the Autonomous System.
Options	A value corresponding to the neighbor's Options field.
Priority	The priority of the neighbor in the designated router election algorithm. A value of 0 indicates that the neighbor is not eligible to become the designated router on this particular network. This is a value between 0 and 255.
State	The state of the relationship with this neighbor.
Events	The number of times this neighbor relationship has changed state or an error has occurred.
RetransmissionQueueLength	The current length of the retransmission queue.
NbmaNbrPermanence	The status of the entry. The values *dynamic* and *permanent* refer to how the neighbor came to be known.
HelloSuppressed	This field indicates whether Hello packets are being suppressed to the neighbor.
InterfaceAddr	The neighbor's interface address.

3 Click **Refresh** to update the information.

—End—

Virtual interface information

Use the **Virtual If** tab of the OSPF dialog to view virtual interface information.

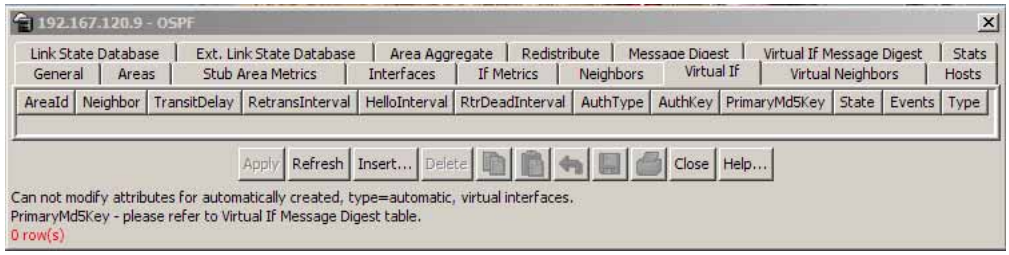
Use the following procedure to view OSPF Virtual Interface information:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog opens.

2 Select the **Virtual If** tab. The **Virtual If** tab is illustrated below.

Virtual If tab



3 Use the fields on the tab, as described in the following table, to view the Virtual Interface information.

Virtual Interface fields

Field	Description
AreaId	Specifies the unique ID of the area connected to the interface. **TIP**: an area ID of 0.0.0.0 indicates the OSPF backbone.
Neighbor	Specifies ID of adjacent, reachable routers.
TransitDelay	Specifies the estimated number of seconds required to transmit a link state update packet over the virtual interface. The transit delay is expressed as an integer between 0 and 3600.
RetransInterval	Specifies the number of seconds between link state advertisement retransmissions for adjacencies belonging to the virtual interface. The retransmit interval is also used to transmit database description and link state request packets. The retransmit interval is expressed as an integer between 0 and 3600.
HelloInterval	Specifies the interval, in seconds, between the Hello packets sent by the router on the virtual interface. **TIP**: This value must be the same for all routers attached to a common network. The hello interval is expressed as an integer between 1 and 65535.

Field	Description
RtrDeadInterval	Specifies the number of seconds since a router last transmitted hello packets before neighbor routers declare it down. The retransmit dead interval is expressed as an integer between 0 and 2147483647. **TIP**: The retransmit dead interval should be a multiple of the hello interval and must be the same for all routers attached to a common network.
AuthType	Specifies the interface authentication type. The available authentication types are: none, simplePassword, or MD5.
AuthKey	Specifies the interface authentication key used with the simplePassword authentication type.
PrimaryMd5Key	Specifies the MD5 primary key. If no MD5 primary key exists, the value in this field is 0.
State	Specifies the current DR state of the interface. States are designated router (DR), backup designated router (BDR), or OtherDR.
Events	Specifies the number of times the virtual interface has changed state or the number of times an error has occurred.
Type	Specifies whether the virtual interface is broadcast or passive.

4 Click one of the labelled buttons across the bottom of the tab to refresh the information in the view, insert or delete information, apply changes, copy or paste settings, reset changes, export information to an external file or print.

—End—

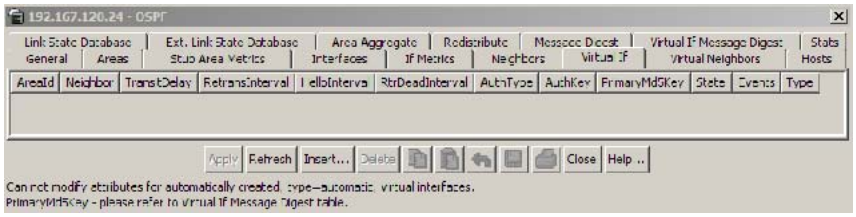
Virtual interface creation

To create an OSPF virtual interface, use the following procedure.

Creating an OSPF virtual interface

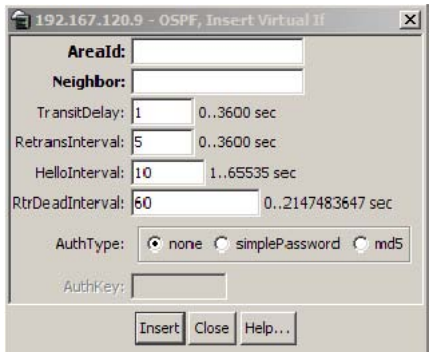
Step	Action
1	From the Device Manager main menu, select **IP Routing**.
2	Select **OSPF**. The OSPF window opens with the General tab open.
3	Select the **Virtual If** tab. The Virtual If window opens.

Virtual interface tab



4 Click **Insert**. The OSPF, Insert Virtual If dialog opens.

Insert virtual interface dialog



5 Enter the information in the fields on the Virtual If window.

OSPF Insert Virtual Interface fields

Field	Description
AreaId	Specifies the unique identifier of the area connected to the interface. **TIP**: an area ID of 0.0.0.0 indicates the OSPF backbone.
Neighbor	Specifies the ID of adjacent, reachable routers.
TransitDelay	Specifies the estimated number of seconds required to transmit a link state update packet over the virtual interface. Transit delay is expressed as an integer between 0-3600. The default value is 0.
RetransInterval	Specifies the number of seconds between link state advertisement retransmissions for adjacencies belonging to the virtual interface. The retransmit interval is also used to transmit database description and link state request packets. The retransmit interval is expressed as an interval between 0-3600. The default value is 5.
HelloInterval	Specifies the interval, in seconds, between the Hello packets sent by the router on the virtual interface. **TIP**: This value must be the same for all routers attached to a common network. The hello interval is expressed as an integer between 1-65535. The default value is 10.
RtrDeadInterval	Specifies the number of seconds since a router last transmitted hello packets before neighbor routers declare it down. The retransmit dead interval is expressed as an integer between 0-2147483647. The default value is 60.

Field	Description
AuthType	Specifies the interface authentication type. The available authentication types are: none, simple password, or MD5. If you select simplePassword, you must supply an authorization key.
AuthKey	Specifies the interface authentication key used with the simplePassword authentication type.

6 Click **Insert**.

—End—

Virtual interface deletion

To delete an OSPF virtual interface, use the following procedure.

Deleting an OSPF virtual interface

Step	Action
1	From the Device Manager main menu, select **IP Routing**.
2	Select **OSPF**. The OSPF window opens.
3	Select the **Virtual If** tab.
4	Select an **AreaId** to delete.
5	Click **Delete**.

—End—

Automatic Virtual Link creation

Use the **AutoVirtLinkEnable** box on the OSPF General tab to create an automatic virtual link. For more information about Virtual Link, see "OSPF virtual link" (page 31).

Use the following procedure to create an automatic Virtual Link.

Creating an automatic Virtual Link

Step	Action
1	From the Device Manager main menu, select **IP Routing > OSPF**. The OSPF dialog opens.
2	On the General tab, enter the router ID in the **RouterId** box for one of the end point ABRs.

3 Check the **AutoVirtLinkEnable** box.

4 Click **Apply**.

5 Enter the router ID in the **RouterId** box for the other end point ABR.

6 Check the **AutoVirtLinkEnable** box.

7 Click **Apply**.

—End—

Automatic Virtual Link Deletion

To delete an automatic Virtual Link use the following procedure.

Deleting an automatic Virtual Link

Step	Action
1	From the Device Manager main menu, select **IP Routing > OSPF**. The OSPF dialog opens.
2	On the General tab, enter the router ID in the **RouterId** box for one of the end point ABRs.
3	Deselect the **AutoVirtLinkEnable** box.
4	Click **Apply**.
5	Enter the router ID in the **RouterId** box for the other end point ABR.
6	Deselect the **AutoVirtLinkEnable** box.
7	Click **Apply**.

—End—

Automatic Virtual Links are also removed when the transit area is deleted or when the router is no longer an ABR.

Virtual neighbors information

Use the **Virtual Neighbors** tab of the OSPF dialog to view virtual neighbor information.

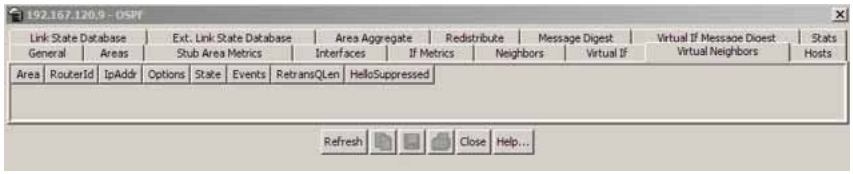
Use the following procedure to view OSPF Virtual Neighbors information:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog opens.

2 Select the **Virtual Neighbors** tab. The **Virtual Neighbors** tab is illustrated below.

Virtual Neighbors tab



3 Use the fields on the tab, as described in the following table, to view the Virtual Neighbors information.

Virtual Neighbors tab fields

Field	Description
Area	Specifies the subnetwork in which the virtual neighbor resides.
RouterId	Specifies the 32-bit integer (represented as a type IpAddress) uniquely identifying the neighboring router in the autonomous system. .
IpAddr	Specifies the IP address of the virtual neighboring router.
Options	Specifies a bit mask corresponding to the option field of the neighbor.
State	Specifies the state of the Virtual Neighbor Relationship.
Events	Specifies the number of state changes or error events that have occurred between the OSPF router and the neighbor router.
RetransQLen	Specifies the current length of the retransmission queue (the number of elapsed seconds between advertising retransmissions of the same packet to a neighbor).
HelloSuppressed	Specifies whether Hello packets to the virtual neighbor are suppressed or not.

4 Click one of the labelled buttons across the bottom of the tab to refresh the information in the view, insert information, copy settings, or print.

—End—

OSPF Hosts information

Use the **Hosts** tab of the OSPF dialog to view virtual neighbor information.

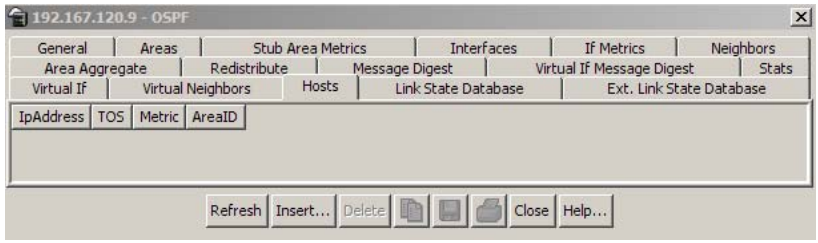
Use the following procedure to view OSPF Hosts information:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog opens.

2 Select the **Hosts** tab. The **Hosts** tab illustration follows.

Hosts tab



3 Use the fields on the tab, as described in the following table, to view the Hosts information.

Hosts fields

Field	Description
IpAddress	Specifies the host IP address.
TOS	Specifies the configured route type of service. **TIP**: the value in this field should be 0 as TOS-based routing is not supported.
Metric	Specifies the configured cost of the host.
AreaID	Specifies the ID of the area connected to the host.

4 Click one of the labelled buttons across the bottom of the tab to refresh the information in the view, insert or delete information, copy settings, export information to an external file, or print.

—End—

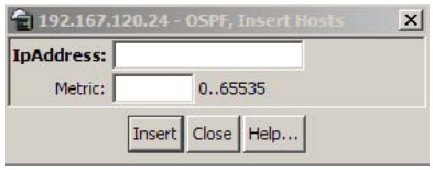
OSPF Host creation

To create an OSPF host, use the following procedure.

Creating an OSPF host

Step	Action
1	From the Device main menu, select **OSPF**. The OSPF window opens.
2	Select the **Hosts** tab. The **Hosts** window opens.
3	Click **Insert**. The **OSPF Insert Hosts** dialog opens.
4	Enter the information on the **Insert Hosts** dialog.

OSPF Insert Hosts dialog



Field	Description
IpAddress	Specifies the host IP address.
Metric	Specifies the configured cost of the host.

5	Click **Insert**.

—End—

OSPF Host deletion

To delete an OSPF host, use the following procedure.

Deleting an OSPF host

Step	Action
1	From the Device Manager main menu, select **OSPF**.
2	Select **Hosts**.
3	Select the **IpAddress** to delete.
4	Click **Delete**.

—End—

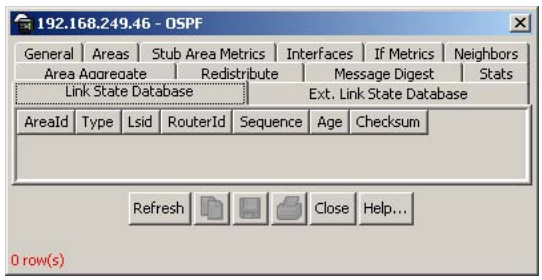
Link State Database information

The **Link State Database** tab of the **OSPF** dialog is used to view link state information. To view OSPF link states, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Link State Database** tab. This tab is illustrated below.

OSPF dialog - Link State Database tab



2 Using the fields provided, view the link state database. These fields are described in the following table.

Link State Database fields

Field	Description
AreaId	The unique identifier of the Area the link state advertisement was received from.
Type	The type of link state advertisement. Each link state type has a separate advertisement format.
Lsid	The Link State ID is a link state type-specific field containing either a Router ID or an IP address. This field identifies the section of the routing domain that is being described by the advertisement.
RouterId	The unique identifier of the originating router in the Autonomous System.
Sequence	This field is used to detect old or duplicate link state advertisements by assigning an incremental number to duplicate advertisements. The higher the sequence number, the more recent the advertisement.

Age	The age of the link state advertisement in seconds.
Checksum	The checksum of the complete content of the advertisement, excluding the *Age* field. This field is excluded so that the advertisement's age can be increased without updating the checksum. The checksum used is the same as that used in ISO connectionless datagrams and is commonly referred to as the *Fletcher checksum*.

3 Click **Refresh** to update the information.

—End—

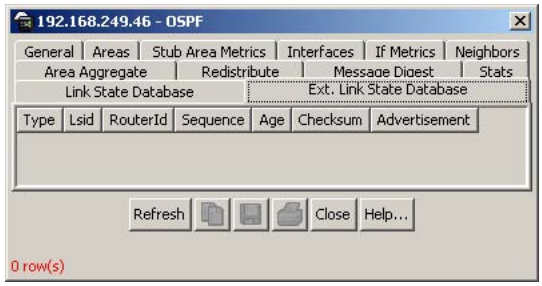
External Link State Database information

The **Ext. Link State Database** tab of the **OSPF** dialog is used to view external link state information. To view OSPF external link states, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Ext. Link State Database** tab. This tab is illustrated below.

OSPF dialog - Ext. Link State Database tab



2 Using the fields provided, view the external link state database. These fields are described in the following table.

Ext. Link State Database fields

Field	Description
Type	The type of link state advertisement. Each link state type has a separate advertisement format.

Lsid	The Link State ID is a link state type-specific field containing either a Router ID or an IP address. This field identifies the section of the routing domain that is being described by the advertisement.
RouterId	The unique identifier of the originating router in the Autonomous System.
Sequence	This field is used to detect old or duplicate link state advertisements by assigning an incremental number to duplicate advertisements. The higher the sequence number, the more recent the advertisement.
Age	The age of the link state advertisement in seconds.
Checksum	The checksum of the complete content of the advertisement, excluding the *Age* field. This field is excluded so that the advertisement's age can be increased without updating the checksum. The checksum used is the same as that used in ISO connectionless datagrams and is commonly referred to as the *Fletcher checksum*.
Advertisement	The entire link state advertisement including the header."

3 Click **Refresh** to update the information.

—End—

Area Aggregate configuration

The **Area Aggregate** tab of the **OSPF** dialog is used to configure area aggregate information. To configure OSPF area aggregates, use the following procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Area Aggregate** tab. This tab is illustrated below.

OSPF dialog - Area Aggregate tab

2 Using the fields provided, configure the area aggregate information. These fields are described in the following table.

Area Aggregate tab fields

Field	Description
AreaID	The unique identifier of the Area this address aggregate is found in.
LsdbType	The type of address aggregate. This field specifies the link state database type that this address aggregate applies to. Select one of the following types: Summary Link, Aggregated Summary Link, nssaExternal link, or Not so Stubby Area Link.
IpAddress	The IP address of the network or subnetwork indicated by the aggregate range.
Mask	The subnet mask that pertains to the network or subnetwork.
Effect	This field indicates the aggregates effect. Subnets subsumed by aggregate ranges either trigger the advertisement of the indicated aggregate (*advertiseMatching* value) or result in the subnet not being advertised at all outside the area. Select one of the following types: AdvertiseMatching (Advertise the aggregate summary LSA with same LSID), DoNotAdvertiseMatching (Suppress all networks that fall within the entire range) or AdvertiseDoNotAggregate (Advertise individual networks).
AdvertiseMetric	The advertisement metric associated with this aggregate. Enter an integer value between 0 and 65535 which represents the Metric cost value for the OSPF area range.

3 Click **Apply**.

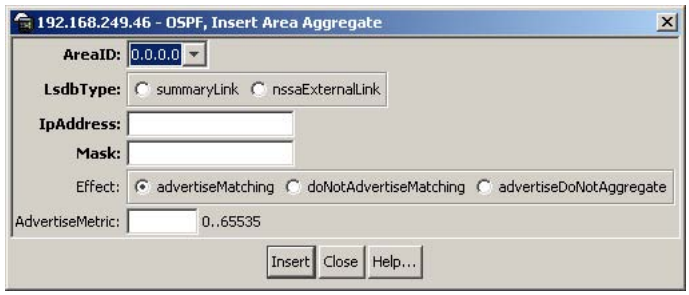
—End—

Area Aggregate creation

To create a new OSPF area aggregate, follow this procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Area Aggregate** tab. This tab is illustrated above.
2	Click **Insert**.
3	The **Insert Area Aggregate** dialog opens. This dialog is illustrated below.

Insert Area Aggregate dialog



Step	Action
4	Using the fields provided, create the new area aggregate. These fields are described in the following table.

Insert Area Aggregate dialog fields

Field	Description
AreaID	The unique identifier of the Area this address aggregate is found in.
LsdbType	The type of address aggregate. This field specifies the link state database type that this address aggregate applies to. Options available are: summaryLink and nssaExternalLink.
IpAddress	The IP address of the network or subnetwork indicated by the aggregate range.
Mask	The subnet mask that pertains to the network or subnetwork.

Effect	This field indicates the aggregates effect. Subnets subsumed by aggregate ranges either trigger the advertisement of the indicated aggregate (*advertiseMatching* value) or result in the subnet not being advertised at all outside the area. Options available are: advertiseMatching, doNotAdvertiseMatching, and advertiseDoNotAggregate.
AdvertiseMetric	The advertisement metric associated with this aggregate. This is an integer value between 0 and 65535.

5 Click **Insert**.

—End—

Area Aggregate deletion

To delete an OSPF area aggregate, use the following procedure.

Deleting an OSPF area aggregate

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **OSPF**. The OSPF dialog opens.
3	Select the **Area Aggregate** tab. The Area Aggregate window opens.
4	Select an **AreaID** to delete.
5	Click **Delete**.

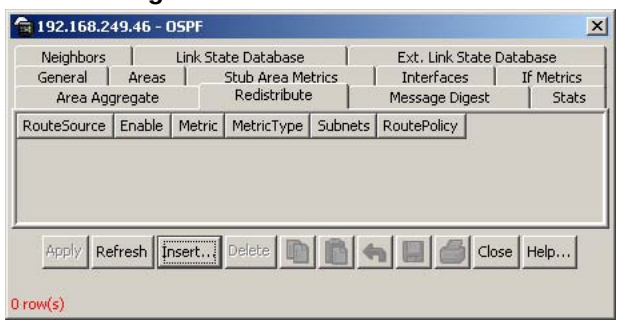
—End—

OSPF redistribution configuration

The **Redistribution** tab of the **OSPF** dialog is used to configure OSPF redistribution settings. To configure OSPF redistribution, use the following procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Redistribute** tab. This tab is illustrated below.

OSPF dialog - Redistribute tab



2 Use the fields provided on this tab to configure redistribution. These fields are described in the following table.

Redistribute tab fields

Field	Description
RouteSource	Select the route source protocol for redistribution (RIP, Direct or Static).
Enable	Indicates whether the redistribution entry is active.
Metric	A value between 0 and 65535 that indicates the metric to be announced in the advertisement.
MetricType	The field specifies the metric type. The value *type1* is treated as an internal metric and *type2* is treated as an external metric.
Subnets	This field indicates whether subnetworks need to be advertised individually. Options available are: allow and suppress.
RoutePolicy	The name of an existing route policy that will be used to determine whether a specific route should be advertised to a given protocol.

3 Click **Apply**.

—End—

Redistribution creation

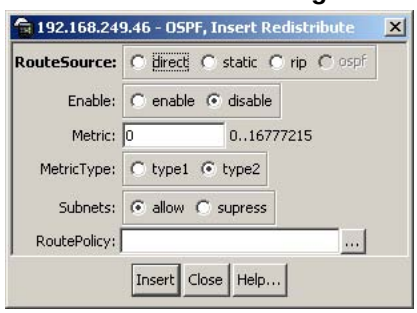
To create a new redistribution entry, follow this procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Redistribute** tab. This tab is illustrated above.

2 Click **Insert**.

3 The **Insert Redistribute** dialog opens. This dialog is illustrated below.

Insert Redistribute dialog



4 Using the fields provided, create the new redistribution entry. These fields are described in the following table.

Insert Redistribute dialog fields

Field	Description
RouteSource	This field indicates that the protocol is either interested or not interested in knowing the routes learned from this source.
Enable	Indicates whether the redistribution entry is active.
Metric	A value between 0 and 65535 that indicates the metric to be announced in the advertisement.
MetricType	The field specifies the metric type. The value *type1* is treated as an internal metric and *type2* is treated as an external metric.
Subnets	This field indicates whether subnetworks need to be advertised individually. Options available are: allow and supress.
RoutePolicy	The name of an existing switch policy that will be used to determine whether a specific route should be advertised to a given protocol.

5 Click **Insert**.

—End—

Redistribution deletion

To delete a redistribution entry, use the following procedure.

Deleting a redistribution entry

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **OSPF**. The OSPF dialog opens.
3	Select the **Redistribute** tab. The Redistribute window opens.
4	Select a **RouteSource** to delete.
5	Click **Delete**.

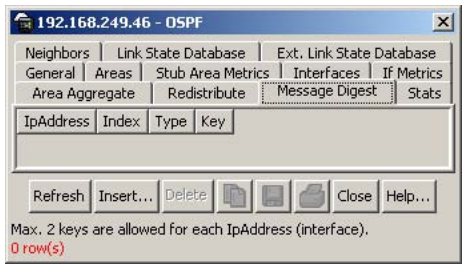
—End—

Message Digest information

The **Message Digest** tab of the **OSPF** dialog is used to view OSPF message digest settings. To view OSPF message digests, use the following procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Message Digest** tab. This tab is illustrated below.

OSPF dialog - Message Digest tab



Step	Action
2	Using the fields provided, view the message digest information. These fields are described in the following table.

Message Digest tab fields

Field	Description
IpAddress	The IP address associated with the digest entry.
Index	The index value of the digest entry. This is an integer value between 1 and 255.

Type	The type of digest entry. Only MD5 is supported.
Key	The key value associated with the digest entry.

3 Click **Refresh** to update the displayed information.

—End—

Message Digest creation

To create a new OSPF message digest entry, follow this procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Message Digest** tab. This tab is illustrated above.
2	Click **Insert**.
3	The **Insert Message Digest** dialog opens. This dialog is illustrated below.

Insert Message Digest dialog

4 Using the fields provided, create the new digest entry. These fields are described in the following table.

Insert Message Digest dialog fields

Field	Description
IpAddress	The IP address associated with the digest entry.
Index	The index value of the digest entry. This is an integer value between 1 and 255.
Type	The type of digest entry. Only MD5 is supported.
Key	The key value associated with the digest entry.

5 Click **Insert**.

—End—

Message Digest deletion

To delete an OSPF message digest entry, use the following procedure.

Deleting an OSPF message digest entry

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **OSPF**. The OSPF dialog opens.
3	Select the **Message Digest** tab. The Message Digest window opens.
4	Select an **IpAddress** to delete.
5	Click **Delete**.

—End—

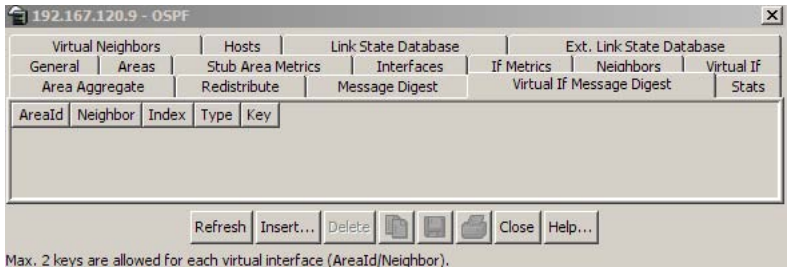
Virtual If Message Digest information

Use the **Virtual If Message Digest** tab of the **OSPF** dialog to view OSPF virtual message digest settings.

To view OSPF virtual message digest settings, use the following procedure:

Step	Action
1	Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog opens.
2	Select the **Virtual If Message Digest** tab. See the following illustration of Virtual If Message Digest tab

Virtual If Message Digest tab



3 Use the fields in the following table to view Virtual If Message Digest information:

Virtual If Message Digest fields

Field	Description
AreaId	Specifies the ID of the area associated with the virtual interface message digest entry.
Neighbor	Specifies the IP address of the neighbor router associated with the virtual interface message digest entry.
Index	Specifies the index value of the virtual interface message digest entry. The value is an integer between 1 and 255.
Type	Specifies the type of virtual interface digest entry.
Key	Specifies the key associated with the virtual interface message digest entry.

4 Click one of the labelled buttons across the bottom of the tab to refresh the information in the view, insert or delete information, copy settings, export information to an external file, or print.

—End—

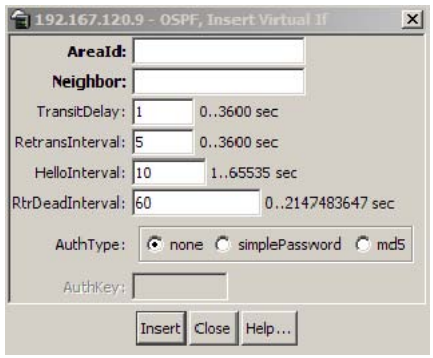
Virtual If Message Digest creation

To create a Virtual Message Digest entry, use the following procedure.

Creating a Virtual If Message Digest entry

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **OSPF**. The OSPF window opens.
3	Select the **Virtual If Message Digest** tab. The Virtual If Message Digest screen opens.
4	Click **Insert**. The OSPF, Insert Virtual If Message Digest window opens.

OSPF Insert Virtual If Message Digest window



5 Enter the information in the fields provided.

6 Click **Insert**.

—End—

Virtual If Message Digest deletion

To delete a Virtual Message Digest entry, use the following procedure.

Deleting a Virtual If Message Digest entry

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **OSPF**. The OSPF dialog opens.
3	Select the **Virtual If Message Digest** tab. The Virtual If Message Digest window opens.
4	Select an **AreaId** to delete.
5	Click **Delete**.

—End—

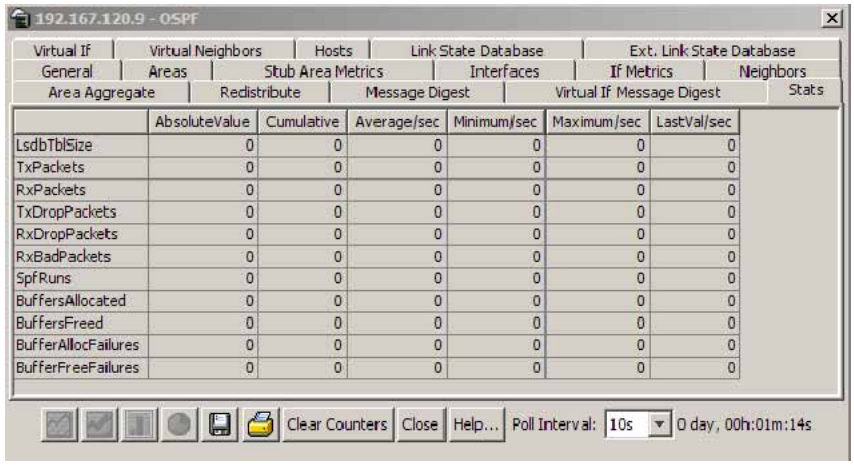
OSPF statistics

The **Stats** tab of the **OSPF** dialog is used to view OSPF statistics. To view OSPF statistics, use the following procedure:

Step	Action

1 Select **IP Routing > OSPF** from the Device Manager menu. The **OSPF** dialog will open. Select the **Stats** tab. This tab is illustrated below.

OSPF dialog Stats tab



2 Using the fields provided, view the OSPF statistics. These fields are described in the table below.

Stats tab fields

Field	Description
LsdbTblSize	Indicates the number of entries in the link state database.
TxPackets	Indicates the number of packets transmitted by OSPF.
RxPackets	Indicates the number of packets received by OSPF.
TxDropPackets	Indicates the number of packets dropped by OSPF before transmission.
RxDropPackets	Indicates the number of packets dropped before receipt by OSPF.
RxBadPackets	Indicates the number of bad packets received by OSPF.
SpfRuns	Indicates the total number of SPF calculations performed. This also includes the number of partial route table calculations.
BuffersAllocated	Indicates the total number of buffers allocated for OSPF.

BuffersFreed	Indicates the total number of buffers that are freed by OSPF.
BufferAllocFailures	Indicates the number of times that OSPF has failed to allocate buffers.
BufferFreeFailures	Indicates the number of times that OSPF has failed to allocate buffers.

3 Values on the *Stats* tab will refresh automatically based on the value selected in the **Poll Interval** field. To clear the counters and start over at zero, click **Clear Counters**.

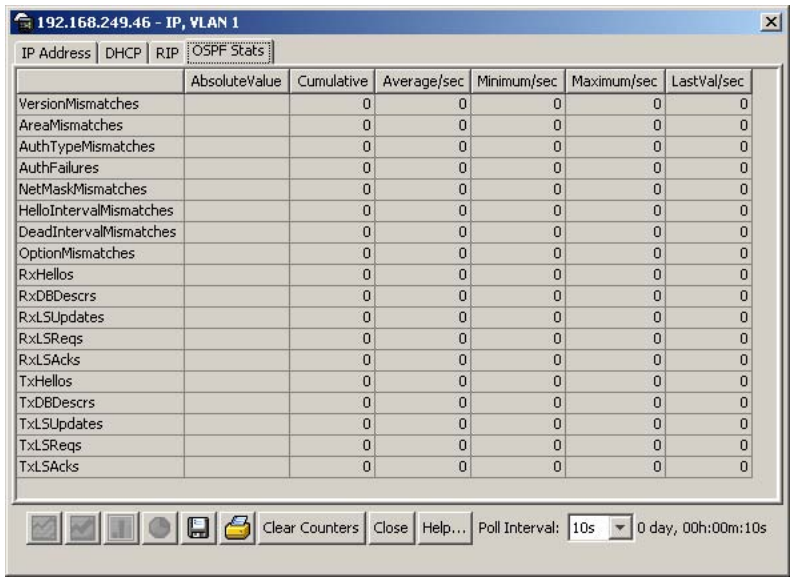
—End—

VLAN OSPF statistics

OSPF statistical information can also be viewed on a per-interface basis. To view VLAN OSPF statistics, perform the following procedure:

Step	Action
1	Select **VLAN > VLANs** from the Device Manager menu. The **VLAN** dialog opens.
2	Select an interface from those listed on the **Basic** tab.
3	Click the **IP** button.
4	On the **IP VLAN** dialog, select the **OSPF Stats** tab. This tab is illustrated below.

OSPF Stats tab



5 The following table describes the fields on this tab.

OSPF Stats tab fields

Field	Description
VersionMismatches	The number of version mismatches received by this interface.
AreaMismatches	The number of area mismatches received by this interface.
AuthTypeMismatches	The number of AuthType mismatches received by this interface.
AuthFailures	The number of authentication failures on this interface.
NetMaskMismatches	The number of net mask mismatches received by this interface.
HelloIntervalMismatches	The number of hello interval mismatches received by this interface.
DeadIntervalMismatches	The number of dead interval mismatches received by this interface.
OptionMismatches	The number of option mismatches received by this interface.
RxHellos	The number of hello packets received by this interface.
RxDBDescrs	The number of database descriptor packets received by this interface.
RxLSUpdates	The number of link state update packets received by this interface.
RxLSReqs	The number of link state request packets received by this interface.
RxLSAcks	The number of link state acknowledge packets received by this interface.

TxHellos	The number hello packets transmitted by this interface.
TxDBDescrs	The number of database descriptor packets transmitted by this interface.
TxLSUpdates	The number of link state update packets transmitted by this interface.
TxLSReqs	The number of link state request packets transmitted by this interface.
TxLSAcks	The number of link state acknowledge packets transmitted by this interface.

—End—

To graph the statistical information, select the desired data and click the appropriate graph button at the bottom of the screen.

Route policies

Route policies are a Nortel proprietary improvement on existing routing schemes. Using existing routing schemes, packets are forwarded based on routes that have been learned by the router through routing protocols such as RIP and OSPF or through the introduction of static routes. Route policies introduce the ability to forward packets based on rule sets created by the network administrator. These rule sets, or policies, are then applied to the learned or static routes.

This section describes the configuration and management of route policies using the Java Device Manager.

Prefix List configuration

The **Prefix List** tab is used for the configuration of policy prefix lists. Prefix lists are the base item in a routing policy. Prefix lists contain lists of IP addresses with their associated masks that support the comparison of ranges of masks.

To configure a prefix list, following this procedure:

Step	Action
1	Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog opens with the **Prefix List** tab selected. This tab is illustrated below.

Policy dialog - Prefix List tab

2 Using the fields provided, configure the selected Prefix List. These fields are described in the following table.

Prefix List tab fields

Field	Description
Id	The unique identifier of this prefix list.
Prefix	The IP address associated with this prefix list.
PrefixMaskLen	The subnet mask length associated with this prefix list.
Name	The name associated with this prefix list.
MaskLenFrom	The mask length from the stated subnet mask.
MaskLenUpto	The mask length up to the stated subnet mask.

3 Click **Apply**.

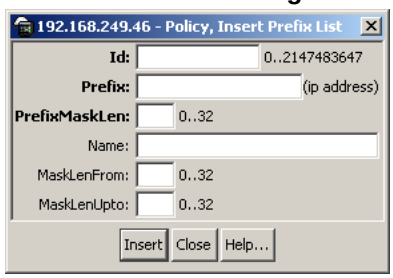
—End—

Prefix List creation

To create a new prefix list, follow this procedure:

Step	Action
1	Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog opens with the **Prefix List** tab selected. This tab is illustrated above.
2	Click **Insert**.
3	The **Insert Prefix List** dialog opens. This dialog is illustrated below.

Insert Prefix List dialog



4 Using the fields provided, create a new prefix list. These fields are described in the following table.

Insert Prefix List dialog fields

Field	Description
Id	The unique identifier of this prefix list.
Prefix	The IP address associated with this prefix list.
PrefixMaskLen	The subnet mask length associated with this prefix list.
Name	The name associated with this prefix list.
MaskLenFrom	The mask length from the stated subnet mask.
MaskLenUpto	The mask length up to the stated subnet mask.

5 Click **Insert**.

—End—

Prefix List deletion

To delete a prefix list, use the following procedure.

Deleting a Prefix List

Step	Action
1	Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog opens with the **Prefix List** tab selected.
2	Select an Id to delete.
3	Click **Delete**.

—End—

Route Policy configuration

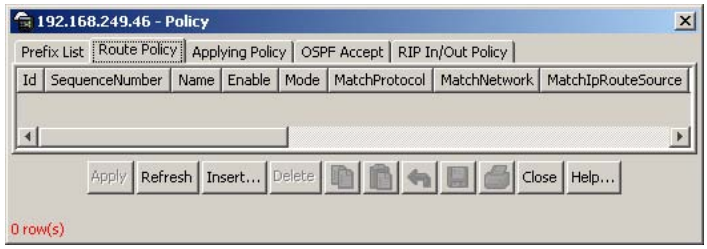
The Route Policy tab is used to configure route policies on the switch. Route policies are created and then applied to switch in either an accept (in), announce (out), or redistribution capacity.

To configure route policies on the switch, perform the following procedure:

Step	Action

1 Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog will open with the **Prefix List** tab selected. Select the **Route Policy** tab. This tab is illustrated below.

Policy dialog - Route Policy tab



2 Using the fields provided, configure the route policy. These fields are described in the following tab.

Route Policy tab fields

Field	Description
Id	The index value used to uniquely identify a group of policies.
SequenceNumber	The secondary index value assigned to individual policies inside a larger policy group.
Name	The name associated with this policy.
Enable	Indicates whether the policy is enabled. Disabled policies should not be used for routing.
Mode	Specifies the action to be taken when this policy is selected for a specific route. A value of **permit** indicates that the route will be used while **deny** indicates that the route will be ignored.
MatchProtocol	Select the appropriate protocol (RIP, Static, Direct, OSPF or Any). If configured, matches the protocol through which the route is learned. This field is used only for RIP announce purposes.
MatchNetwork	If configured, the switch matches the destination network against the contents of the specified prefix list.

MatchIpRouteSource	If configured, matches the next hop IP address for RIP routes and advertising router IDs for OSPF routes against the contents of the specified prefix list. This option is ignored for all other route types.
MatchNextHop	If configured, matches the next hop IP address of the route against the contents of the specified prefix list. This field applies only to non-local routes.
MatchInterface	If configured, the switch matches the IP address of the interface by which the RIP route was learned against the contents of the specified prefix list. This field is used only for RIP routes and ignored for all other type of route.
MatchRouteType	Sets a specific route-type to be matched (applies only to OSPF routes). Externaltype1, and Externaltype2 specify the OSPF routes of the specified type only. OSPF internal refers to intra- and inter-area routes.
MatchMetric	If configured, the switch matches the metric of the incoming advertisement or existing route against the specified value (1 to 655535). If 0, then this field is ignored. The default is 0.
NssaPbit	Set or reset the P bit in specified type 7 LSA. By default the P bit is always set in case the user set it to a disable state for a particular route policy than all type 7. LSAs associated with that route policy will have the P bit cleared with this intact NSSA ABR will not perform translation of these LSAs to type 5. Default is enabled.
SetRoutePreference	Setting the preference greater than zero, specifies the route preference value to be assigned to the routes which matches this policy. This applies to Accept policies only. You can set a value from 0 to 255. The default value is 0. If the default is configured, the global preference value is used.
SetMetric	If configured, the switch sets the metric value for the route while announcing or redistributing. The default-import-metric is 0. If the default is configured, the original cost of the route is advertised into OSPF; for RIP, the original cost of the route or the default value is used.

SetMetricType	Applicable to OSPF protocol only. If configured, sets the metric type for the routes to be announced into the OSPF routing protocol that matches this policy. The default is type 2. This field is applicable only for OSPF announce policies.
SetInjectNetList	If configured, the switch replaces the destination network of the route that matches this policy with the contents of the specified prefix list.
SetMask	Indicates the mask to used for routes that pass the policy matching criteria.

3 Click **Apply**.

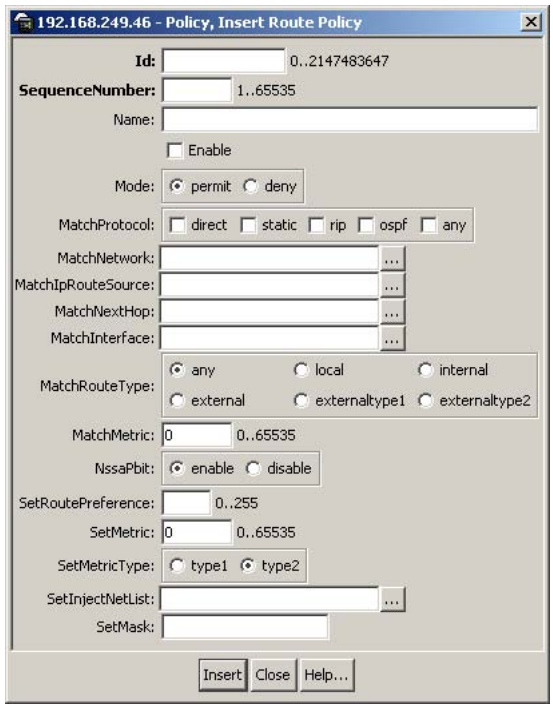
—End—

Route Policy creation

To create a new route policy, follow this procedure:

Step	Action
1	Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog will open with the **Prefix List** tab selected. Select the **Route Policy** tab. This tab is illustrated above.
2	Click **Insert**.
3	The **Insert Route Policy** dialog opens. This dialog is illustrated below.

Insert Route Policy dialog



4 Using the fields provided, create the new route policy. These fields are described in the following table.

Insert Route Policy fields

Field	Description
Id	The index value used to uniquely identify a group of policies.
SequenceNumber	The secondary index value assigned to individual policies inside a larger policy group.
Name	The name associated with this policy.
Enable	Indicates whether the policy is enabled. Disabled policies should be used for routing.
Mode	Specifies the action to be taken when this policy is selected for a specific route. A value of **permit** indicates that the route will be used while **deny** indicates that the route will be ignored.
MatchProtocol	Select the appropriate protocol (RIP, Static, Direct, OSPF or Any). If configured, matches the protocol through which the route is learned. This field is used only for RIP announce purposes.

MatchNetwork	If configured, the switch matches the destination network against the contents of the specified prefix list.
MatchIpRouteSource	If configured, matches the next hop IP address for RIP routes and advertising router IDs for OSPF routes against the contents of the specified prefix list. This option is ignored for all other route types.
MatchNextHop	If configured, matches the next hop IP address of the route against the contents of the specified prefix list. This field applies only to non-local routes.
MatchInterface	If configured, the switch matches the IP address of the interface by which the RIP route was learned against the contents of the specified prefix list. This field is used only for RIP routes and ignored for all other type of route.
MatchRouteType	Sets a specific route-type to be matched (applies only to OSPF routes). Externaltype1, and Externaltype2 specify the OSPF routes of the specified type only. OSPF internal refers to intra- and inter-area routes.
MatchMetric	If configured, the switch matches the metric of the incoming advertisement or existing route against the specified value (1 to 655535). If 0, then this field is ignored. The default is 0.
NssaPbit	Set or reset the P bit in specified type 7 LSA. By default the P bit is always set in case the user set it to a disable state for a particular route policy than all type 7. LSAs associated with that route policy will have the P bit cleared with this intact NSSA ABR will not perform translation of these LSAs to type 5. Default is enabled.
SetRoutePreference	Setting the preference greater than zero, specifies the route preference value to be assigned to the routes which matches this policy. This applies to Accept policies only. You can set a value from 0 to 255. The default value is 0. If the default is configured, the global preference value is used.

SetMetric	If configured, the switch sets the metric value for the route while announcing or redistributing. The default-import-metric is 0. If the default is configured, the original cost of the route is advertised into OSPF; for RIP, the original cost of the route or the default value is used.
SetMetricType	Applicable to OSPF protocol only. If configured, sets the metric type for the routes to be announced into the OSPF routing protocol that matches this policy. The default is type 2. This field is applicable only for OSPF announce policies.
SetInjectNetList	If configured, the switch replaces the destination network of the route that matches this policy with the contents of the specified prefix list.
SetMask	Indicates the mask to used for routes that pass the policy matching criteria.

5 Click **Insert**.

—End—

Route policy deletion

To delete a route policy, use the following procedure.

Deleting a route policy

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **Policy**. The Policy dialog opens.
3	Select the **Route Policy** tab.
4	Select an Id to delete.
5	Click **Delete**.

—End—

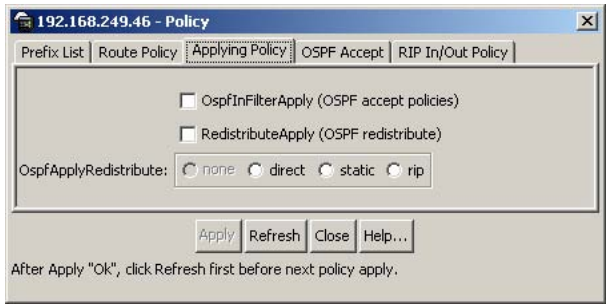
Applying OSPF policies

The Applying Policy tab is used to apply configured OSPF policies to the switch. To configure policy application, perform the following procedure:

Step	Action

1 Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog opens with the **Prefix List** tab selected. Select the **Applying Policy** tab. This tab is illustrated below.

Policy dialog - Applying Policy tab



2 Using the fields provided, select the policies to be applied. These fields are described in the following table.

Applying Policy tab fields

Field	Description
OspfInFilterApply	Select this check box to apply OSPF accept policies.
RedistributeApply	Select this check box to apply OSPF redistribution policies.
OspfApplyRedistribute	If applying OSPF redistribution policies, select the type of redistribution from the available options.

3 Click **Apply**.

—End—

OSPF Accept Policy configuration

The **OSPF Accept** tab is used to configure OSPF accept policies on the switch. To configure OSPF accept policies, perform the following tasks:

Step	Action

1 Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog opens with the **Prefix List** tab selected. Select the **OSPF Accept** tab. This tab is illustrated below.

Policy dialog - OSPF Accept tab

2 Using the fields provided, configure the desired accept policy. These fields are described in the following table.

OSPF Accept tab fields

Field	Description
AdvertisingRtr	The advertising router associated with the accept policy.
Enable	Indicates whether the policy is enabled.
MetricType	Indicates the metric type associated with the policy. Available options are: type1, type2, and any.
PolicyName	Indicates the name associated with the policy.

3 Click **Apply**.

—End—

OSPF Accept Policy creation

To create a new OSPF accept policy, follow this procedure:

Step	Action

1 Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog opens with the **Prefix List** tab selected. Select the **OSPF Accept** tab. This tab is illustrated above.

2 Click **Insert**.

3 The **Insert OSPF Accept** dialog opens. This dialog is illustrated below.

Insert OSPF Accept dialog

4 Using the fields provided, create the new accept policy. These fields are described in the following table.

Insert OSPF Accept fields

Field	Description
AdvertisingRtr	The advertising router associated with the accept policy.
Enable	Indicates whether the policy is enabled.
MetricType	Indicates the metric type associated with the policy. Available options are: type 1, type 2, and any.
PolicyName	Indicates the name associated with the policy.

5 Click **Insert**.

—End—

OSPF Accept Policy deletion

To delete an OSPF accept policy, use the following procedure.

Deleting an OSPF accept policy

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **Policy**. The Policy dialog appears.
3	Select the **OSPF Accept** tab. The OSPF Accept window opens.
4	Select an **AdvertisingRtr** to delete.
5	Click **Delete**.

—End—

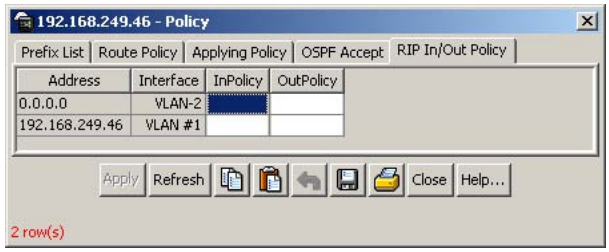
RIP In and Out Policy configuration

The **RIP In/Out Policy** tab is used to configure RIP accept and announce policies on switch interfaces. To configure these policies, follow this procedure:

Step	Action

1 Select **IP Routing > Policy** from the Device Manager menu. The **Policy** dialog opens with the **Prefix List** tab selected. Select the **RIP In/Out Policy** tab. This tab is illustrated below.

Policy dialog - RIP In/Out Policy tab



2 Using the fields provided, configure the RIP policies. These fields are described in the following table.

RIP In/Out Policy tab fields

Field	Description
Address	The address of the RIP interface.
Interface	The associated switch interface.
InPolicy	A previously configured policy that will be used as the accept policy on this interface.
OutPolicy	A previously configured policy that will be used as the announce policy on this interface.

3 Click **Apply**.

—End—

Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure that can occur when the single static default gateway router for an end station is lost.

This section describes the procedures used to configure VRRP using the Java Device Manager.

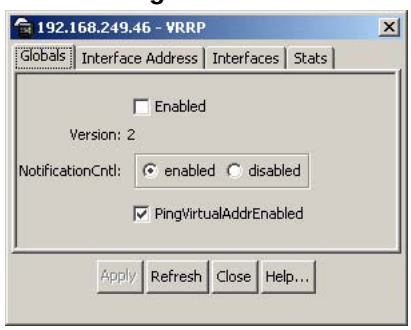
Global VRRP configuration

The Device Manager can be used to configure global VRRP settings. This is done from the VRRP **Globals** tab.

To configure global VRRP settings, use the following procedure:

Step	Action
1	Select **IP Routing > VRRP** from the Device Manager menu. The **VRRP** dialog opens with the **Globals** tab selected. This tab is illustrated below.

VRRP dialog - Globals tab



Step	Action
2	Using the provided fields, configure the global VRRP settings. These fields are illustrated in the following table.

Globals tab fields

Field	Description
Enabled	Indicates whether VRRP is globally enabled on the switch.
Version	Indicates the version of VRRP supported on this switch.

NotificationCntl	Indicates whether the VRRP-enabled router generates Simple Network Management Protocol (SNMP) traps based on VRRP events: • Enabled - SNMP traps are sent. • Disabled - SNMP traps are not sent.
PingVirtualAddrEnabled	Indicates whether this device should respond to pings directed to a virtual router's IP address.

3 Click **Apply**.

—End—

VRRP interface creation

The **Interface Address** tab of the **VRRP** dialog is used to create new VRRP interfaces. Configuration and management of these interfaces is performed on the **Interfaces** tab.

To create new VRRP interfaces, use the following procedure:

Step	Action

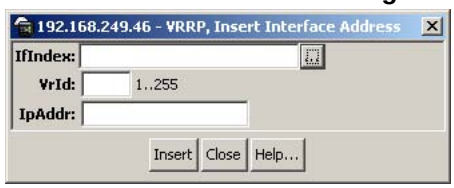
1 Select **IP Routing > VRRP** from the Device Manager menu. The **VRRP** dialog opens with the **Globals** tab selected. Select the **Interface Address** tab. This tab is illustrated below.

VRRP dialog - Interface Address tab

2 Click **Insert**.

3 The Insert Interface Address dialog opens. This dialog is illustrated below.

Insert Interface Address dialog



4 Using the provided fields, create the new interface. These fields are outlined in the following table.

Insert Interface Address dialog fields

Field	Description
IfIndex	The interface index to assign to the new interface. Click the button at the end of the field to select a previously configured interface. Otherwise, enter an index value directly.
VrId	The virtual router ID to assign to this interface.
IpAddr	The IP address to assign to this interface.
Status	The status of the interface; active or inactive.

5 Click **Insert**.

—End—

VRRP Interface deletion

To delete a VRRP interface, use the following procedure.

Deleting a VRRP interface

Step	Action
1	From the Device Manager menu, select **IP Routing**. The IP Routing menu appears.
2	Select **VRRP**. The VRRP window opens.
3	Select the **Interface Address** tab. The Interface Address window opens.
4	Select an IfIndex to delete.
5	Click **Delete**.

—End—

VRRP interface management

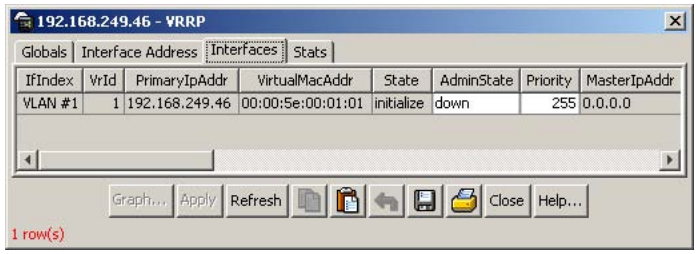
The **Interfaces** tab is used to manage VRRP interfaces created on the **Interface Address** tab.

To manage VRRP interfaces, use the following procedure:

Step	Action

1 Select **IP Routing > VRRP** from the Device Manager menu. The **VRRP** dialog opens with the **Globals** tab selected. Select the **Interfaces** tab. This tab is illustrated below.

VRRP dialog - Interfaces tab



2 Manage VRRP interfaces using the provided fields. These fields are outlined in the following table.

Interfaces tab fields

Field	Description
IfIndex	The interface index of the VRRP interface.
VrId	A number that uniquely identifies a virtual router on a given VRRP router.
PrimaryIpAddr	An IP address selected from the set of real interface addresses. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.
VirtualMacAddr	The virtual MAC address of the virtual router.
State	The current state of the virtual router. A virtual router can be in one of the following states: **initalize** (indicates the virtual router is waiting for a startup event), **backup** (indicates the virtual router is monitoring the availability of the master router), or **master**\ (indicates the virtual router is forwarding packets for IP addresses associated with the router).

AdminState	Indicates the administrative status of the virtual router.
Priority	Indicates the priority to be used for the virtual router master election process. This is an integer value between 1 and 255. The priority value for the VRRP router that owns the IP addresses associated with the virtual router must be 255. The default priority value for VRRP routers backing up a virtual router is 100.
MasterIpAddr	Indicates the master router's real (primary) IP address. This is the IP address listed as the source in the VRRP advertisement last received by this virtual router.
AdvertisementInterval	Indicates the time interval, in seconds, between transmission of advertisement messages. Only the master router sends VRRP advertisements. This is an integer value between 1 and 255. The default value is 1.
VirtualRouterUpTime	Indicates the amount of time this virtual router has spent out of the **initialize** state.
HolddownTimer	The amount of time (in seconds) to wait before preempting the current VRRP master. This is an integer value between 0 and 21600.
HoldDownState	The holddown state of this VRRP interface.
HoldDownTimeRemaining	The amount of time (in seconds) left before the holddown timer will expire.
Action	Used to trigger an action on this VRRP interface. Options available are: none (no action) or preemptHoldDownTimer.
CriticalIpAddrEnabled	Indicates whether the user-defined critical IP address is enabled. If the user-defined critical IP address is not enabled, a default critical IP address of 0.0.0.0 will be used.
CriticalIpAddr	The IP address of the interface that will cause a shutdown event.
BackupMasterEnabled	Indicates whether the backup/master functionality is enabled on this interface.

BackupMasterState	Indicates the state of the backup/master functionality.
FastAdvertisementEnabled	Indicates if the Faster Advertisement Interval should be used. The default value is false.
FastAdvertisementInterval	The fast advertisement interval, in milliseconds, between sending advertisement messages. This is an integer value between 200 and 1000. The default value is 200.

3 Click **Apply**.

—End—

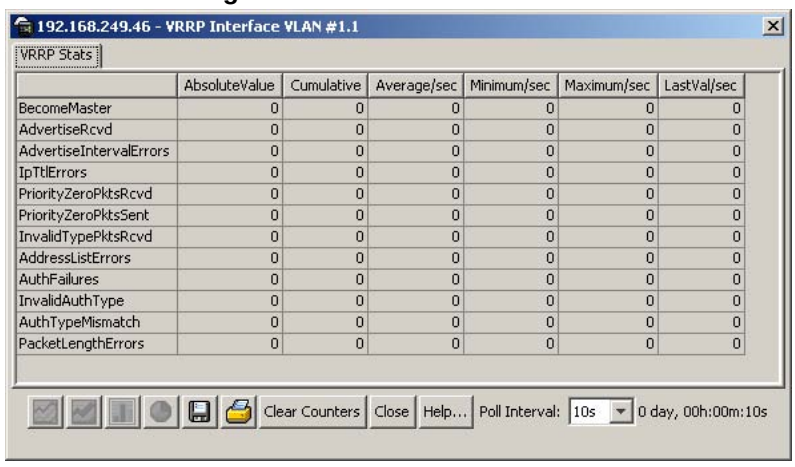
Graphing VRRP interface information

Statistical information about the VRRP interface can be viewed and graphed on the **Interfaces** tab.

To view and graph this statistical information, use the following procedure:

Step	Action
1	Select **IP Routing > VRRP** from the Device Manager menu. The **VRRP** dialog opens with the **Globals** tab selected. Select the **Interfaces** tab. This tab is illustrated above.
2	Select a listed interface and click **Graph**.
3	The **VRRP Stats** dialog opens. This dialog is illustrated below.

VRRP Stats dialog



4 Using the provided fields, view and graph the VRRP statistical information. The following table outlines these fields

VRRP Stats fields

Field	Description
BecomeMaster	The total number of times that this virtual router's state has transitioned to MASTER.
AdvertiseRcvd	The total number of VRRP advertisements received by this virtual router.
AdvertiseIntervalErrors	The total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router.
IpTtlErrors	The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
PriorityZeroPktsRcvd	The total number of VRRP packets received by the virtual router with a priority of 0.
PriorityZeroPktsSent	The total number of VRRP packets sent by the virtual router with a priority of 0.
InvalidTypePktsRcvd	The number of VRRP packets received by the virtual router with an invalid value in the **type** field.
AddressListErrors	The total number of packets received for which the address list does not match the locally configured list for the virtual router.
AuthFailures	The total number of VRRP packets received that do not pass the authentication check.
InvalidAuthType	The total number of packets received with an unknown authentication type.
AuthTypeMismatch	The total number of packets received with **Auth Type** not equal to the locally configured authentication method.
PacketLengthErrors	The total number of packets received with a packet length less than the length of the VRRP header.

—End—

Viewing general VRRP statistics

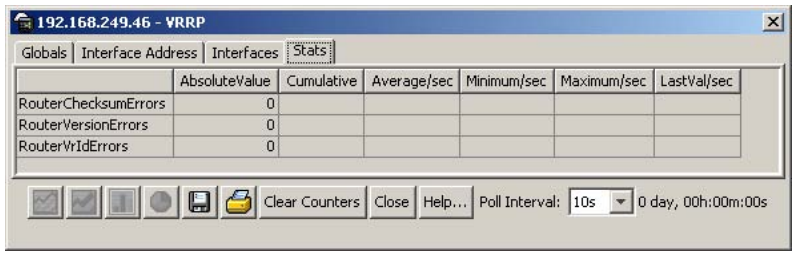
General VRRP statistics can be viewed and graphed on the **Stats** tab.

To view and graph general VRRP statistics, use the following procedure:

Step	Action

1 Select **IP Routing > VRRP** from the Device Manager menu. The **VRRP** dialog opens with the **Globals** tab selected. Select the **Stats** tab. This tab is illustrated below.

VRRP dialog - Stats tab



2 Using the provided fields to view and graph the general VRRP statistics. The following table outlines these fields.

Stats tab fields

Field	Description
RouterChecksumErrors	The total number of VRRP packets received with an invalid VRRP checksum value.
RouterVersionErrors	The total number of VRRP packets received with an unknown or unsupported version number.
RouterVrIdErrors	The total number of VRRP packets received with an invalid VRID for this virtual router.

—End—

Equal Cost MultiPath (ECMP)

The Equal Cost MultiPath (ECMP) feature allows routers to determine equal cost paths to the same destination prefix. The multiple paths can be used for load sharing of traffic and allows faster convergence to other active paths in case of network failure. This section describes the procedures used to configure ECMP on the switch using the Java Device Manager.

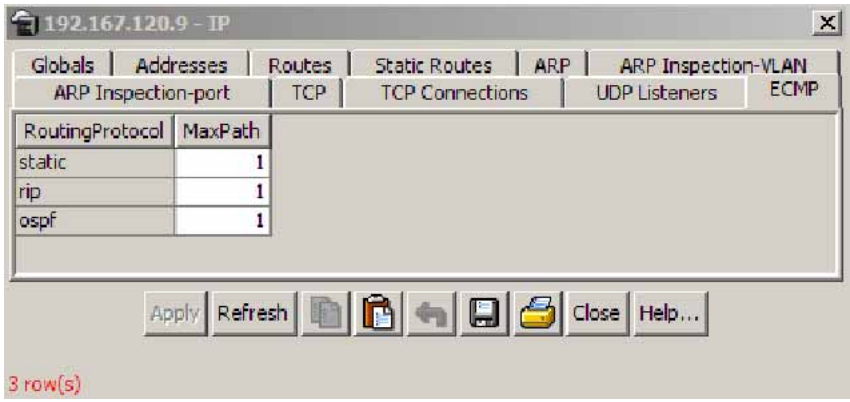
Note: ECMP is only supported on the Nortel Ethernet Routing Switch 5520 and 5530. ECMP will work in a mixed stack but will not run on any Nortel Ethernet Routing Switch 5510 units in the stack.

ECMP configuration

The **ECMP** tab is used to configure and manage ECMP settings for RIP, OSPF, and static routes.

To configure ECMP, use the following procedure:

Step	Action
1	Select **IP Routing > IP** from the Device Manager menu. The **IP** dialog opens with the **Globals** tab selected. Select the **ECMP** tab. This tab is illustrated below.



2	Using the **MaxPath** field, enter the number of paths allotted to each protocol listed. Up to 4 paths can be allotted to each. The default is 1.
3	Click **Apply**.

—End—

Brouter port

A brouter port is a single-port VLAN that can route IP packets as well as bridge all non-routable traffic. The following section describes the procedures necessary to configure and manage brouter ports on the Nortel Ethernet Routing Switch 5500 Series using the Java Device Manager.

Configuration and management of Brouter ports

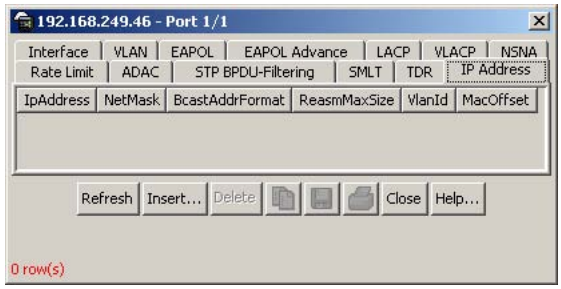
The **IP Address** tab of the **Port** dialog is used to configure and manage the switch brouter ports.

To configure and manage brouter ports, use the following procedure:

Step	Action
1	Select a port on the Device Manager **Front Panel** view.

2 Select **Edit > Port** from the Device Manager menu. The **Port** dialog opens with the **Interface** tab selected. Select the **IP Address** tab. This tab is illustrated below.

Port dialog - IP Address tab



3 Use the provided fields to view the brouter port settings. These fields are outlined in the following table.

IP Address tab fields

Field	Description
IpAddress	The IP address assigned to this brouter.
NetMask	The subnet mask associated with the brouter IP address.
BcastAddrFormat	The IP broadcast address format used on this interface.
ReasmMaxSize	The size of the largest IP datagram which this entity can reassemble from incoming IP fragmented datagrams received on this interface.
VlanId	The VLAN ID associated with this brouter port.
MacOffset	The MAC address offset associated with this brouter port.

—End—

Creating a Brouter port

To create a new brouter port, use the following procedure:

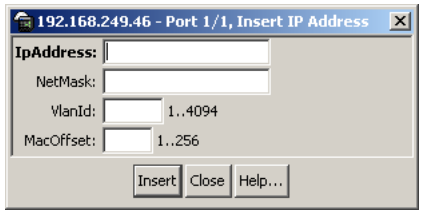
Step	Action
1	Select a port on the Device Manager **Front Panel** view.

2 Select **Edit > Port** from the Device Manager menu. The **Port** dialog opens with the **Interface** tab selected. Select the **IP Address** tab. This tab is illustrated above.

3 Click **Insert**.

4 The **Insert IP Address** dialog opens. This dialog is illustrated below.

Insert IP Address dialog



5 Using the provided fields, create the new brouter port. These fields are outlined in the following table.

Insert IP Address dialog fields

Field	Description
IpAddress	The IP address assigned to this brouter.
NetMask	The subnet mask associated with the brouter IP address.
VlanId	The VLAN ID associated with this brouter port.
MacOffset	The MAC address offset associated with this brouter port.

6 Click **Insert**.

—End—

Note: Brouter ports are treated as routable VLANs and are displayed on the **Basic** tab of the **VLANs** screen.

Deleting a Brouter port

To delete a brouter port, use the following procedure:

Step	Action
1	Select a port on the Device Manager **Front Panel** view.
2	Select **Edit > Port** from the Device Manager menu. The **Port** dialog opens with the **Interface** tab selected. Select the **IP Address** tab.

3 Select a brouter port from these listed on the tab by clicking in the row.

4 Click **Delete**.

—End—

UDP broadcast forwarding

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address. This section outlines the procedures used to configure and manage UDP broadcast forwarding using the Java Device Manager.

UDP protocol configuration

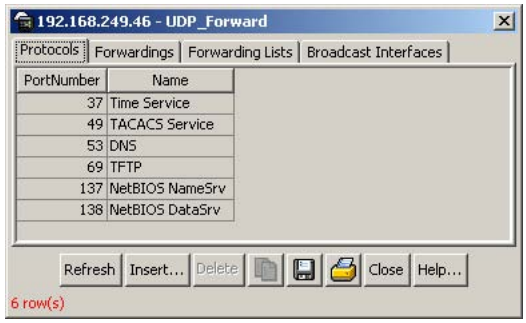
The **Protocols** tab of the **UDP Forward** dialog is used to define UDP ports for use in UDP forwarding.

To configure a UDP port, use the following procedure:

Step	Action

1 Select **IP Routing > UDP Forwarding** from the Device Manager menu. The **UDP Forwarding** dialog opens with the **Protocols** tab selected. This tab is illustrated below.

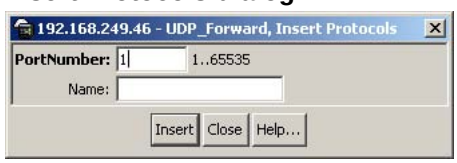
UDP Forward dialog - Protocols tab



2 Click **Insert**.

3 The **Insert Protocols** dialog opens. This dialog is illustrated below.

Insert Protocols dialog



4 Using the provided fields, configure the new UDP protocol. These fields are outlined in the following table.

Insert Protocols dialog fields

Field	Description
PortNumber	The port the new UDP protocol will use.
Name	The name associated with the UDP protocol.

5 Click **Insert**.

—End—

UDP forwarding configuration

The **Forwardings** tab of the **UDP Forward** dialog is used to assign a server IP address to a previously configured protocol.

To configure a UDP forwarding, use the following procedure:

Step	Action

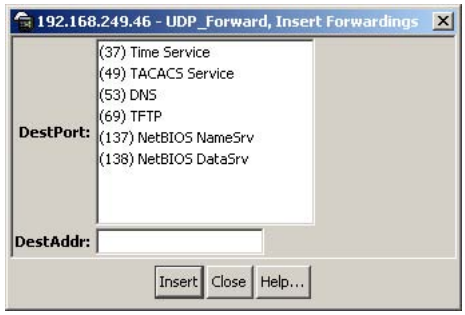
1 Select **IP Routing > UDP Forwarding** from the Device Manager menu. The **UDP Forwarding** dialog opens with the **Protocols** tab selected. Select the **Forwardings** tab. This tab is illustrated below.

UDP Forward dialog - Forwardings tab

2 Click **Insert**.

3 The **Insert Forwardings** dialog opens. This dialog is illustrated below.

Insert Forwardings dialog



4 Using the provided fields, configure the UDP forwarding. These fields are outlined in the following table.

Insert Forwardings dialog fields

Field	Description
DestPort	The destination port of the UDP forwarding. These are configured on the **Protocols** tab.
DestAddr	The server IP address.

5 Click **Insert**.

—End—

UDP forwarding deletion

To delete a server IP address from a previously configured protocol, use the following procedure.

Deleting a UDP forwarding

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP Routing menu appears.
2	Select **UDP Forwarding**. The UDP Forwarding dialog opens.
3	Select the **Forwardings** tab.
4	Select a DestPort to delete.
5	Click **Delete**.

—End—

UDP forwarding list configuration

The **Forwarding Lists** tab of the **UDP Forward** dialog is used to group the port/server IP pairs configured on the **Forwardings** tab into lists and assign name to the lists.

To configure a forwarding list, use the following procedure:

Step	Action

1 Select **IP Routing > UDP Forwarding** from the Device Manager menu. The **UDP Forwarding** dialog opens with the **Protocols** tab selected. Select the **Forwarding Lists** tab. This tab is illustrated below.

UDP Forward dialog - Forwarding Lists tab

2 Using the provided fields, configure the forwarding list. These fields are outlined in the following table.

Forwarding Lists tab fields

Field	Description
Id	The unique identifier assigned to the forwarding list.
Name	The name assigned to the forwarding list.
FwdIdList	The identifiers of the port/server IP pairs created on the **Forwardings** tab and associated with the forwarding list.

3 Click **Apply**.

—End—

UDP forwarding list creation

To create a new forwarding list, use the following procedure:

Step	Action

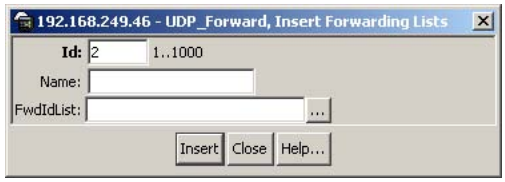
1 Select **IP Routing > UDP Forwarding** from the Device Manager menu. The **UDP Forwarding** dialog opens with the **Protocols** tab

selected. Select the **Forwarding Lists** tab. This tab is illustrated above.

2 Click **Insert**.

3 The **Insert Forwarding Lists** dialog opens. This dialog is illustrated below.

Insert Forwarding Lists dialog



4 Using the provided fields, configure the new forwarding list. These fields are outlined in the following table.

Insert Forwarding Lists dialog fields

Field	Description
Id	The unique identifier assigned to the forwarding list.
Name	The name assigned to the forwarding list.
FwdIdList	The identifiers of the port/server IP pairs created on the **Forwardings** tab and associated with the forwarding list.

5 Click **Insert**.

—End—

UDP forwarding list deletion

To delete a UDP forwarding list, use the following procedure.

Deleting a UDP forwarding list

Step	Action
1	From the Device Manager menu, select **IP Routing** . The **IP Routing** menu appears.
2	Select **UDP Forwarding**. The **UDP Forwarding** dialog opens with the **Protocols** tab selected.
3	Select the **Forwarding Lists** tab.

4 Select an Id to delete.

5 Click **Delete**.

—End—

Configuring UDP broadcast interfaces

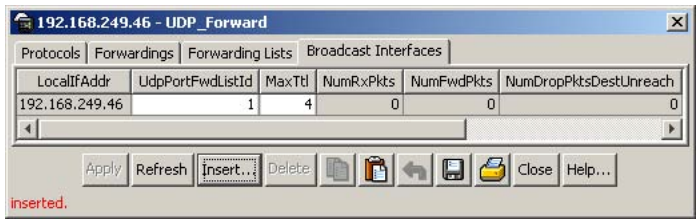
The **Broadcast Interfaces** tab is used to assign a forwarding list to an interface. The TTL for outgoing packets and the broadcast mask for incoming packets are also added on this tab.

To configure the broadcast interface, use the following procedure:

Step	Action

1 Select **IP Routing > UDP Forwarding** from the Device Manager menu. The **UDP Forwarding** dialog opens with the **Protocols** tab selected. Select the **Broadcast Interfaces** tab. This tab is illustrated below.

UDP Forward dialog - Broadcast Interfaces tab



2 Using the provided fields, configure the broadcast interface. These fields are outlined in the following table.

Broadcast Interface tab fields

Field	Description
LocalIfAddr	The IP address of the local interface.
UdpPortFwdListId	The port forwarding lists associated with the interface. This ID is defined in the **Forwarding Lists** tab.
MaxTtl	Indicates the maximum number of hops an IP broadcast packet can take from the source device to the destination device. This is an integer value between 1 and 16.
NumRxPkts	The total number of UDP broadcast packets received by this local interface.
NumFwdPkts	The total number of UDP broadcast packets forwarded.

NumDropPktsDestUnreach	The total number of UDP broadcast packets dropped because the destination was unreachable.
NumDropPktsUnknownPort	The total number of UDP broadcast packets dropped because the destination port or protocol specified has no matching forwarding policy.
BroadCastMask	The subnet mask of the local interface that is used for broadcasting the UDP broadcast packets.

3 Click **Apply**.

—End—

UDP broadcast interface creation

To create a new broadcast interface, use the following procedure:

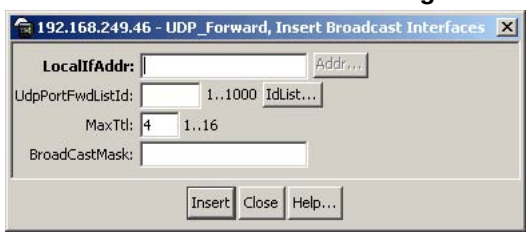
Step	Action

1 Select **IP Routing > UDP Forwarding** from the Device Manager menu. The **UDP Forwarding** dialog opens with the **Protocols** tab selected. Select the **Broadcast Interfaces** tab. This tab is illustrated above.

2 Click **Insert**.

3 The **Insert Broadcast Interface** dialog opens. This dialog is illustrated below.

Insert Broadcast Interfaces dialog



4 Using the provided fields, create the new broadcast interface. These fields are outlined in the following table.

Insert Broadcast Interfaces dialog fields

Field	Description
LocalIfAddr	The IP address of the local interface.
UdpPortFwdListId	The port forwarding lists associated with the interface. This ID is defined in the **Forwarding Lists** tab.
MaxTtl	Indicates the maximum number of hops an IP broadcast packet can take from the source device to the destination device. This is an integer value between 1 and 16.
BroadCastMask	The subnet mask of the local interface that is used for broadcasting the UDP broadcast packets.

5 Click **Insert**.

—End—

UDP broadcast interface deletion

To delete a UDP broadcast interface, use the following procedure.

Deleting a UDP broadcast interface

Step	Action
1	From the Device Manager main menu, select **IP Routing**. The IP routing menu appears.
2	Select **UDP Forwarding**. The UDP Forwarding dialog opens.
3	Select the **Broadcast Interfaces** tab. The Broadcast Interfaces window opens.
4	Select a LocalIfAddr to delete.
5	Click **Delete**.

—End—

DHCP configuration

The following topics describe DHCP configuration using the Device Manager.

DHCP Relay

Use the **DHCP relay** tab to view and configure the DHCP settings for the switch.

To view the **DHCP Relay** tab, select **IP Routing > DHCP** from the Device Manager menu. The following figure illustrates the **DHCP Relay** tab.

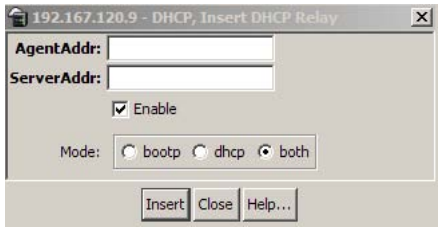
DHCP Relay tab

To configure a DHCP entry, use the following procedure:

Creating a DHCP entry

Step	Action
1	From the Device Manager, select **IP Routing > DHCP**. The **DHCP Relay** tab appears.
2	Click the **Insert** button. The DHCP, Insert DHCP Relay dialog, as illustrated in the following figure, appears.

Insert DHCP Relay



Step	Action
3	Make the new DHCP progressRelay entry in the fields provided. The following table describes the fields in the **Insert DHCP Relay** dialog.

Insert DHCP Relay fields

Field	Description
AgentAddr	The IP address configured on an interface.
ServerAddr	The IP address of the DHCP server. This IP address should be a remote address, so the DHCP packet is sent through unicast to the remote device.
Enable	Enables the DHCP mode.
Mode	Indicate whether this entry pertains to BOOTP packets, DHCP packets, or both.

4 Click **Insert**. The new DHCP entry displays on the **DHCP Relay** screen.

—End—

To delete a DHCP entry, use the following procedure.

Deleting a DHCP entry

Step	Action
1	From the Device Manager, select **IP Routing > DHCP**. The **DHCP Relay** tab appears.
2	Select a DHCP relay entry to delete.
3	Click **Delete**.

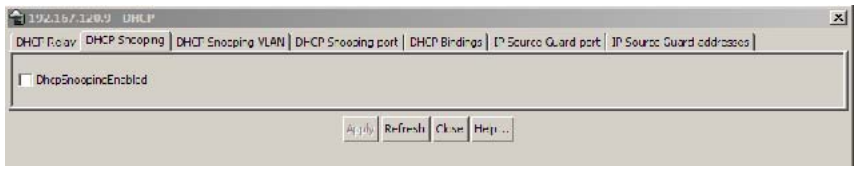
—End—

DHCP Snooping

To enable DHCP Snooping, use the following procedure.

Step	Action
1	From the Device Manager menu, select **IP Routing > DHCP**. The DHCP window appears.
2	Select the **DHCP Snooping** tab. DHCP Snooping dialog appears.

DHCP Snooping tab



3	To enable DHCP Snooping, click the check box. The status appears.
4	Click **Apply**.

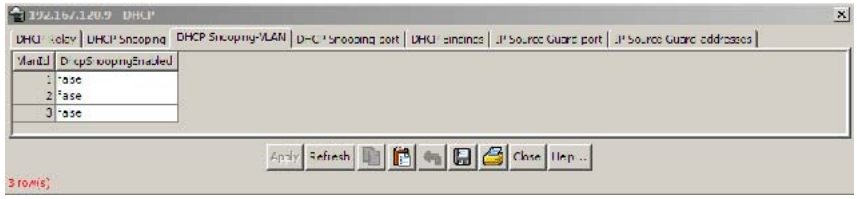
—End—

DHCP Snooping VLAN

To view DHCP Snooping information for VLANs, use the following procedure.

Step	Action
1	From the Device Manager menu, select **IP Routing > DHCP**. The **DHCP** window appears.
2	Select the **DHCP Snooping-VLAN** tab. The **DHCP Snooping-VLAN** window appears. If DHCP Snooping is enabled for a VLAN the field is true. If DHCP Snooping is disabled for a VLAN, the field is false.

DHCP Snooping-VLAN tab



3	Select a VlanId.
4	To change the status, double click the DhcpSnoopingEnabled box for the VLAN.
5	Select **true** or **false**.
6	Click **Apply**.

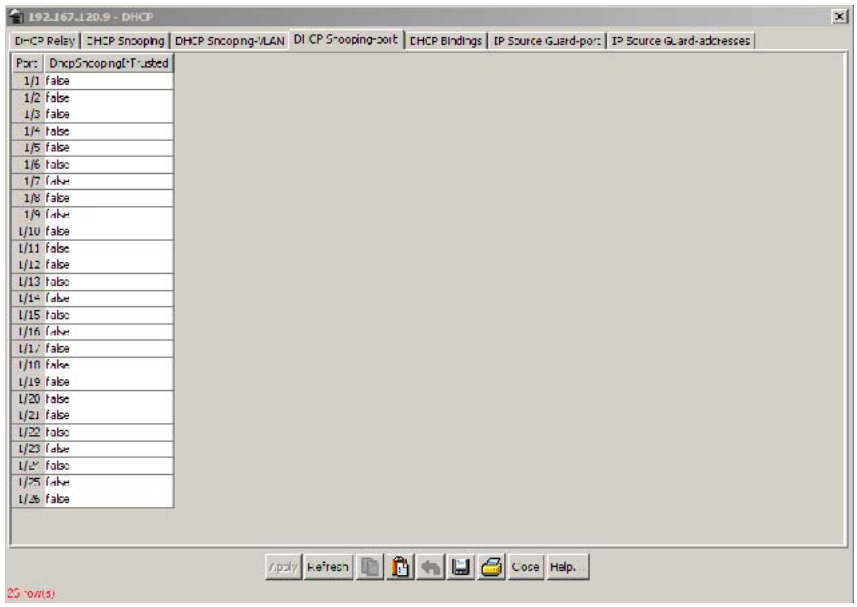
—End—

DHCP Snooping port

To view DHCP Snooping information for ports, use the following procedure.

Step	Action
1	From the Device Manager menu, select **IP Routing > DHCP**. The **DHCP** window appears.
2	Select the **DHCP Snooping-port** tab. The **DHCP Snooping-port** window appears.

DHCP Snooping-port tab



3 Select a port.

4 To change the status, double click the DhcpSnoopingIfTrusted box for the port.

Note: The DhcpSnoopingIfTrusted field value is used to control whether this interface is trusted for DHCP snooping purposes.

5 Select **true** or **false**.

6 Click **Apply**.

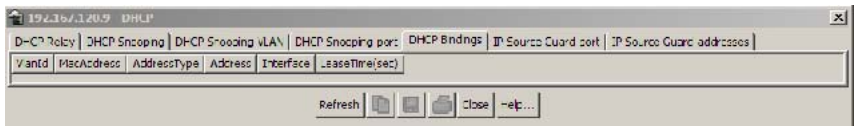
—End—

DHCP bindings

To view information about learned DHCP bindings, use the following procedure.

Step	Action
1	From the Device Manager menu, select **IP Routing > DHCP**. The **DHCP** window appears.
2	Select the **DHCP Bindings** tab. The **DHCP Bindings** window appears.

DHCP Bindings



—End—

The following table describes the fields in the DHCP Bindings window.

Field	Description
VlanId	Specifies the VLAN ID for the DHCP client..
MacAddress	Specifies the VLAN MAC address for the DHCP client.
AddressType	Specifies the type of address contained in the corresponding binding address.
Address	Specifies the IP address for the DHCP client.
Interface	Specifies the interface to which the DHCP client is connected.
LeaseTime(sec)	Specifies the DHCP client binding lease time, in seconds.

IP Source Guard port

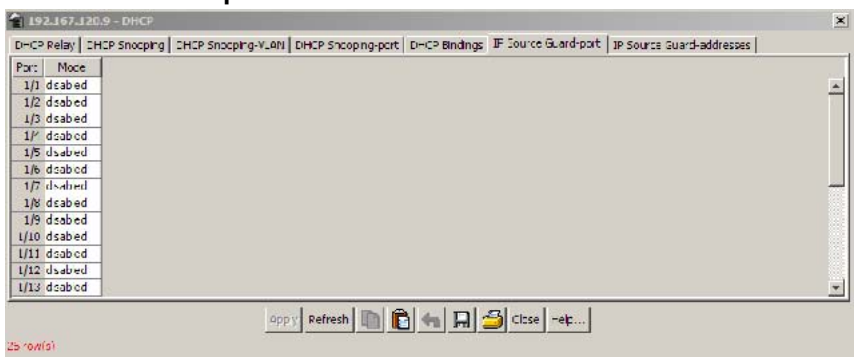
To view IP Source Guard status for ports, use the following procedure.

Step	Action
1	From the Device Manager menu, select **IP Routing > DHCP**. The **DHCP Relay** window appears.

DHCP Relay tab

2	Select the IP Source Guard-port tab. The **IP Source Guard-port** window appears.

IP Source Guard-port tab



3 To change the port mode, select a port.

4 Double click the mode box.

5 Select **ip** or **disabled**.

6 Click **Apply**.

—End—

IP Source Guard addresses

To view IP Source Guard address information, use the following procedure.

Step	Action

1 From the Device Manager menu, select **IP Routing > DHCP**. The **DHCP Relay** window opens.

2 Select the **IP Source Guard-addresses** tab. The **IP Source Guard-addresses** window appears.

IP Source Guard-addresses tab

—End—

The following table describes the fields in the IP Source Guard-addresses window:

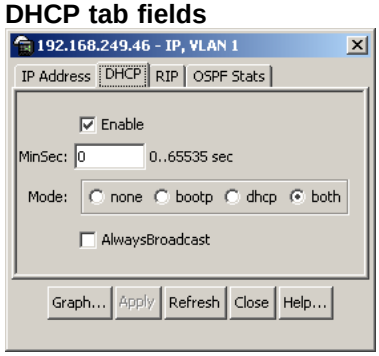
Field	Description
Port	Specifies the IP Source Guard-enabled port number.
Type	Specifies the port type.
Address	Specifies the IP address allowed to communicate with the port. **TIP**: Up to 10 IP addresses are allowed on an IP Source Guard-enabled port. Traffic from other addresses is dropped.
Source	Specifies the address source.

VLAN DHCP configuration

DHCP can also be configured for Layer 3 VLANs. To configure DHCP for a Layer 3 VLAN, follow this procedure:

Step	Action
1	Open the **VLANs** screen by selecting **VLAN > VLANs** from the JDM menu.
2	Highlight the VLAN for which DHCP is to be configured.
3	Click **IP**. The **IP VLAN** screen opens. Select the **DHCP** tab. This tab is illustrated below.

DHCP tab fields



The following table describes the DHCP tab fields.

DHCP tab fields

Fields	Description
Enable	Specifies whether DHCP is enabled or disabled.

Fields	Description
MinSec	Indicates the minimum number of seconds to wait between receiving a DHCP packet and actually forwarding the DHCP packet to the destination device. A value of zero(0) indicates forwarding should be done immediately without any delay.
Mode	Indicates what type of DHCP packets this interface supports. A value of none(1) results in all incoming DHCP and BOOTP packets being dropped.
AlwaysBroadcast	Indicates if DHCP Reply packets should be broadcast to the DHCP client on this interface.

4 Make changes as necessary in the fields provided.

5 Click **Apply**.

—End—

Note: A procedure for viewing and graphing DHCP statistics can be found in *Nortel Ethernet Routing Switch Configuration - System Monitoring* Part Number NN47200-505

Configuring IGMP snooping using the Java Device Manager

This section describes the methods and procedures to configure and manage IGMP snooping using the Java Device Manager. For more information, refer to "IGMP snooping" (page 46)

To enable IGMP Snooping for a VLAN, use the following procedure.

Enabling IGMP Snooping for a VLAN

Step	Action
1	From the Device Manager main menu, select **>VLAN**. The VLAN dialog opens.
2	Select the **Snoop** tab. The Snoop dialog opens.

VLAN Snoop tab

Step	Action
3	Select a VLAN.
4	To enable snooping, double click the **Enable** field for the VLAN and select **true**.
5	To enable proxy reporting, double click the field and select **true**.
6	To change other field values, click the field and enter the value.
7	Click **Apply** to commit the configuration changes.

—End—

TIP: You can change the presentation order of the VLANs in the Snoop table. Click the column name of any column. An up or down arrow, indicating ascending or descending order, appears next to the column name.

VLAN Snoop tab fields

Field	Description
Id	The number assigned to the VLAN during creation.
Name	The VLAN name.
Enable	Specifies snooping status: • if **false**, snooping is disabled • if **true**, snooping is enabled
ReportProxyEnable	Specifies the IGMP report proxy status. • if **false**, no proxy report generates • if **true**, a proxy report (IGMP host membership report) generates The default ReportProxyEnable setting is **false** (disabled).
Robustness	Specifies the robust value. Use a Robustness value to tune the system for the expected packet loss on a subnet. ***Note:*** If a subnet experiences unacceptably high packet losses, increase the Robustness value. The default Robustness value is 2.
QueryInterval	Specifies the query time, in seconds, between IGMP host and query packets transmitted on an interface. QueryInterval, the time between general queries sent by the multicast router, controls the number of IGMP messages allowed on the subnet The default setting is 125 seconds.
MRouterPorts	Displays the set of ports in the VLAN providing connectivity to an IP multicast router.
Ver1MRouterPorts	Displays the set of ports in the VLAN providing connectivity to an IP Multicast router using IGMP version 1.
Ver2MRouterPorts	Displays the set of ports in the VLAN providing connectivity to an IP Multicast router using IGMP version 2.
ActiveMRouterPorts	Displays the set of active ports in the VLAN providing connectivity to an IP Multicast router.
ActiveQuerier	Displays the IP address of a multicast querier router.

Field	Description
QuerierPort	Displays the port on which the multicast querier router was heard.
MRouterExpiration	Displays the multicast querier router aging timeout value.

Configuring IGMP using Web-based management

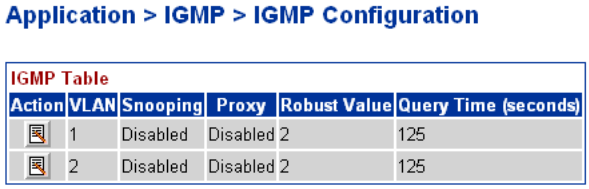
This chapter describes the methods and procedures for the configuration and management of IGMP.

Configuring IGMP using the Web-based Management Interface

The Web-based Management Interface provides tools for the configuration and management of IGMP. To configure IGMP using these tools, use the following procedure:

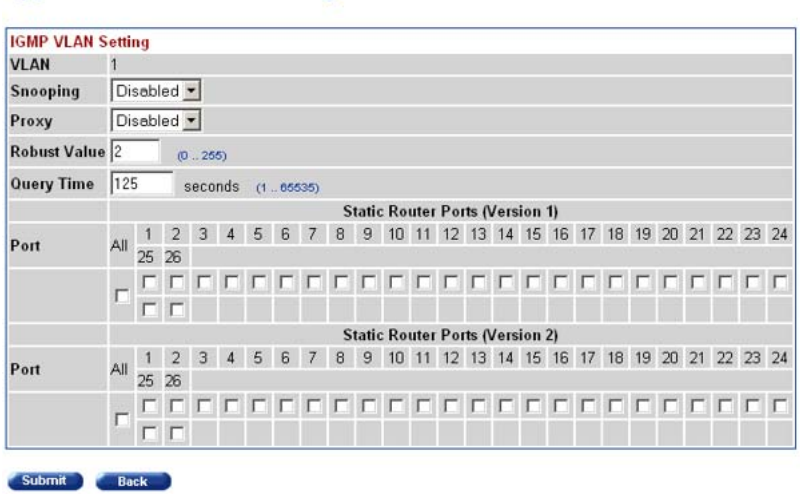
Step	Action
1	Open the IGMP Configuration window by choosing **Applications > IGMP > IGMP Configuration** from the menu.

IGMP Configuration screen



2	Click the icon in the **Action** column beside the VLAN for the IGMP to be configured. The IGMP: VLAN Configuration window appears.

IGMP: VLAN Configuration screen



3 In the fields provided in the **IGMP VLAN Setting** window, configure IGMP for the VLAN. The following table outlines the fields in this window.

IGMP VLAN Setting fields

Field	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
Snooping	Select to enable or disable the IGMP snooping feature. ***Note:*** This field affects only the VLAN specified in the page's VLAN field. The default setting is Disabled.

Field	Description
Proxy	Select to enable or disable the Proxy feature. This feature lets the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. ***Note:*** This field affects *only* the VLAN specified in the page's VLAN field. The default setting is Disabled.
Robust Value	Type the robust value in the appropriate format. This feature lets you set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. ***Note:*** This field affects *only* the VLAN specified in the page's VLAN field. The default setting is 2.
Query Time	Type the query time (in seconds) in the appropriate format. This feature lets you control the number of IGMP messages allowed on the subnet by varying the query interval (the interval between general queries sent by the multicast router). ***Note:*** This field affects *only* the VLAN specified in the page's VLAN field. The default setting is 125 seconds.
Static Router Ports (Version 1 and Version 2)	Select the check boxes of the router ports to associate with the VLAN (alternatively, select the check box to uncheck a selected router port).

Field	Description
	Note: This field affects *only* the VLAN specified in the page's VLAN field.

4 Click **Submit**.

—End—

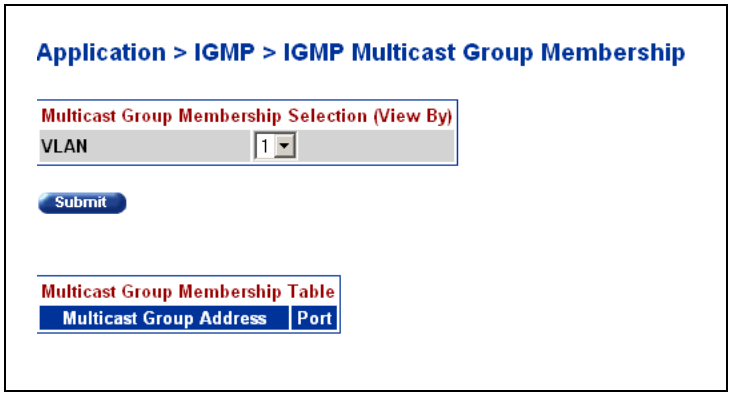
The VLAN Configuration screen reopens and the settings are saved.

Displaying multicast membership using the Web-based Management Interface

Use the following procedure to display Multicast membership in the Web-based Management Interface:

Step	Action
1	Open the IGMP Multicast Group Membership window by choosing **Applications > IGMP > Multicast Group** from the menu.

IGMP Multicast Group Membership window



2 Select the VLAN whose membership is to be viewed from the **VLAN** list in the **Multicast Group Membership Selection (View By)** section.

3 Click **Submit**.

—End—

The membership information appears in the Multicast Group Membership Table section.

The following table describes the IGMP Multicast Group Membership page fields.

IGMP Multicast Group Membership page fields

Section	Field	Description
Multicast Group Membership Selection (View By)	VLAN	Select the VLAN on which to view configured IP addresses.
Multicast Group Membership Table	Multicast Group Address	The IP Multicast group addresses that are currently active on the associated port.
	Port	The port numbers associated with the IP Multicast group addresses displayed in the IP Multicast Group Address field.

Index

Nortel Ethernet Routing Switch 5500 Series

Configuration-IP Routing Protocols

Publication: NN47200-503
Document status: Standard
Document version: 03.01
Document date: 27 August 2007

To provide feedback, or report a problem in this document, go to http://www.nortel.com/documentfeedback.

Sourced in Canada and the United States of America.

The information in this document is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.